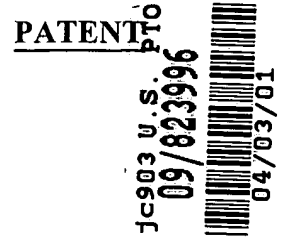


Docket No.: 57454-066



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Tadaaki YAMAUCHI, et al.

Serial No.:

Group Art Unit:

Filed: April 03, 2001

Examiner:

For: SEMICONDUCTOR MEMORY DEVICE INTERNALLY PROVIDED WITH LOGIC
CIRCUIT WHICH CAN BE READILY CONTROLLED AND CONTROLLING
METHOD THEREOF

**CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Commissioner for Patents
Washington, DC 20231

Sir:

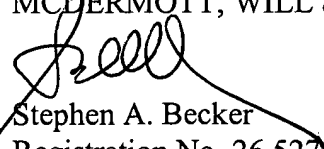
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2000-299012,
filed September 29, 2000

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY


Stephen A. Becker
Registration No. 26,527

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 SAB:dtb
Date: April 3, 2001
Facsimile: (202) 756-8087

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

21454-066
Yamauchi, et al.
April 3, 2001

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年 9月29日

出願番号

Application Number:

特願2000-299012

出願人

Applicant(s):

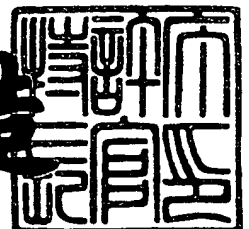
三菱電機株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年10月20日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3087357



【書類名】 特許願

【整理番号】 527098JP01

【提出日】 平成12年 9月29日

【あて先】 特許庁長官殿

【国際特許分類】 G11C 11/34

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社
社内

【氏名】 山内 忠昭

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社
社内

【氏名】 小猿 邦彦

【特許出願人】

【識別番号】 000006013

【氏名又は名称】 三菱電機株式会社

【代理人】

【識別番号】 100064746

【弁理士】

【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132

【弁理士】

【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409

【弁理士】

【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781

【弁理士】

【氏名又は名称】 堀井 豊

【選任した代理人】

【識別番号】 100096792

【弁理士】

【氏名又は名称】 森下 八郎

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 半導体記憶装置および半導体記憶装置の制御方法

【特許請求の範囲】

【請求項 1】 外部から与えられる制御信号、アドレスおよびデータを受ける端子群と、

前記アドレスによって指定される領域に対して前記制御信号に応じて前記データの授受を行なうメモリセルアレイと、

前記メモリセルアレイに対して前記制御信号、前記アドレスおよび前記データが与えられるシーケンスと同じシーケンスで前記端子群に前記制御信号、前記アドレスおよび前記データが与えられた場合に、前記アドレスが所定の第 1 の領域を指定したときに前記制御信号、前記アドレスおよび前記データの少なくともいずれか 1 つに応じてデータ処理を行なうロジック回路とを備える、半導体記憶装置。

【請求項 2】 前記端子群から前記制御信号、前記アドレスおよび前記データを受け、前記アドレスに応じて前記メモリセルアレイと前記ロジック回路のいずれか一方に対して、前記制御信号、前記アドレスおよび前記データの少なくともいずれか 1 つに応じた動作を指示するインターフェイス部をさらに備え、

前記ロジック回路は、

前記インターフェイス部からの指示内容を保持するデータ保持部と、

前記データ保持部の保持内容に応じてデータ処理を行なうデータ処理回路とを含む、請求項 1 に記載の半導体記憶装置。

【請求項 3】 前記指示内容は、

前記データ処理回路の動作を指定するコマンドと、

前記データ処理回路が処理する入力データとを含み、

前記データ保持部は、

前記コマンドを保持する第 1 の保持回路と、

前記入力データを保持する第 2 の保持回路と、

前記入力データを前記データ処理回路がデータ処理した処理結果を保持する第 3 の保持回路とを含む、請求項 2 に記載の半導体記憶装置。

【請求項 4】 前記データ保持部は、

前記データ処理回路がデータ処理を完了したか否かを示すフラグを保持する第 4 の保持回路をさらに含む、請求項 3 に記載の半導体記憶装置。

【請求項 5】 前記データ処理回路は、暗号処理を行ない、

前記入力データは、

暗号の鍵データを含む、請求項 3 に記載の半導体記憶装置。

【請求項 6】 前記指示内容は、

前記データ処理回路の複数の動作モードの指定を含み、

前記データ保持部は、

前記複数の動作モードを保持する保持回路を有し、

前記保持回路は、前記メモリアレイに一回に書込むデータ幅分のビットの容量を有し、

前記ロジック回路に対する前記複数の動作モードの指定は、前記メモリアレイに対する 1 回のデータ書込を行なうシーケンスと同じシーケンスで行なわれる、請求項 2 に記載の半導体記憶装置。

【請求項 7】 前記インターフェイス部は、

前記制御信号に応じて書換え可能なモードレジスタを含み、

前記インターフェイス部は、前記モードレジスタの保持値に応じて前記第 1 の領域をアドレス空間のどこに割当ててくるかを決定する、請求項 2 に記載の半導体記憶装置。

【請求項 8】 前記所定の第 1 の領域は、

前記メモリアレイのアドレス空間の一部の領域である、請求項 1 に記載の半導体記憶装置。

【請求項 9】 前記所定の第 1 の領域は、

前記メモリアレイのアドレス空間以外の仮想的なアドレス空間の一部の領域である、請求項 1 に記載の半導体記憶装置。

【請求項 10】 前記ロジック回路は、仮想的なアドレス空間の一部である前記所定の第 1 の領域へのアクセスに応じて、前記所定の第 1 の領域に対応する前記メモリアレイのアドレス空間に格納されたデータに処理を加える、請求

項 9 に記載の半導体記憶装置。

【請求項 1 1】 外部から与えられる制御信号、アドレスおよびデータを受ける端子群と、前記アドレスによって指定される領域に対して前記制御信号に応じて前記データの授受を行なうメモリセルアレイと、前記メモリセルアレイに対して前記制御信号、前記アドレスおよび前記データが与えられるシーケンスと同じシーケンスで前記端子群に前記制御信号、前記アドレスおよび前記データが与えられた場合に、前記アドレスが所定の第 1 の領域を指定したときに前記制御信号、前記アドレスおよび前記データの少なくともいずれか 1 つに応じてデータ処理を行なうロジック回路とを備える半導体記憶装置の制御方法であって、

前記第 1 の領域を予約領域に指定するステップと、

前記メモリセルアレイへの書込シーケンスと同じシーケンスで前記アドレスによって前記第 1 の領域を指定して前記ロジック回路へのコマンドを与えるステップとを備える、半導体記憶装置の制御方法。

【請求項 1 2】 前記メモリセルアレイへの読出シーケンスと同じシーケンスで前記第 1 の領域を指定して前記ロジック回路の処理結果を読出すステップをさらに備える、請求項 1 1 に記載の半導体記憶装置の制御方法。

【請求項 1 3】 前記半導体記憶装置は、前記端子群を介して、キャッシュメモリを内蔵するマイクロコンピュータと接続され、

前記第 1 の領域を前記キャッシュメモリを使用しない領域として指定するステップをさらに備える、請求項 1 1 に記載の半導体記憶装置の制御方法。

【請求項 1 4】 外部から与えられる制御信号、アドレスおよびデータを受ける第 1 の端子群と、

行列状に配置される複数のメモリセルを含み、外部から与えられる選択信号に応じて活性化され、前記アドレスによって指定される領域に対して前記制御信号に応じて前記データの授受を行なうメモリと、

前記選択信号に応じて前記メモリと相補的に活性化され、前記アドレスおよび前記データの少なくともいずれか 1 つに応じてデータ処理を行なうロジック回路と、

前記選択信号を受ける第 2 の端子とを備える、半導体記憶装置。

【請求項 1 5】 前記メモリは、前記第 1 の端子群に時分割に与えられる行アドレスと列アドレスとを含む前記アドレスに応じて前記メモリセルの選択動作を行ない、

前記ロジック回路は、前記第 1 の端子群に一括して与えられる前記アドレスに応じて動作を行なう、請求項 1 4 に記載の半導体記憶装置。

【請求項 1 6】 前記ロジック回路は、

前記行アドレスと前記列アドレスの変化を検知して動作タイミングを発生する A T D 回路を含む、請求項 1 5 に記載の半導体記憶装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

この発明は、半導体記憶装置に関し、より特定的にはロジック回路を内蔵した半導体記憶装置およびその制御方法に関する。

【 0 0 0 2 】

【従来の技術】

図 5 3 は、従来の、6 4 M b i t の容量を有し、ワード構成が $\times 1 6$ b i t であるシンクロナスダイナミックランダムアクセスメモリ (S D R A M) のピン配置を示した図である。

【 0 0 0 3 】

図 5 4 は、 S D R A M の端子名と機能とを示した図である。

図 5 3、図 5 4 を参照して、従来の S D R A M は、5 4 ピンの端子を有するパッケージに収められており、マスタクロックが入力される端子 C L K、クロックイネーブル信号が入力される端子 C K E、チップセレクト信号が入力される端子 / C S、ロウアドレスストロープ信号が入力される端子 / R A S、コラムアドレスストロープ信号が入力される端子 / C A S、ライトイネーブル信号が入力される端子 / W E を有している。

【 0 0 0 4 】

従来の S D R A M は、さらに、データ入出力信号を授受する端子 D Q 0 ~ D Q 1 5、出力ディスエーブル信号 / ライトマスク信号が入出力される端子 D Q M (

U/L), アドレスが入力される端子A0~A11, バンクアドレスが入力される端子BA0, BA1, 電源が与えられる端子VDD, 出力用電源が与えられる端子VDDQ, 接地電位が与えられる端子VSS, 出力用接地電位が与えられる端子VSSQを有している。

【0005】

これらの端子は、図53に示すように、1番ピンから13番ピンおよび42番ピンから54番ピンの間にデータ入出力端子および電源が配置され、15番ピンから19番ピンおよび37番ピンから39番ピンの間に制御信号およびクロック信号が配置されており、20番ピンから35番ピンの間にアドレス入力ピンが配置されている。このような端子配置は、ある程度汎用性を有しており、メモリを搭載するシステムに用いられる基板にもよく使われている。

【0006】

図55は、従来のロジック内蔵DRAMの構成を示す図である。

図55を参照して、チップ501には、DRAM504とロジック508が搭載されており、DRAMへのアクセス用の制御信号/RAS, /CAS, ..., /CSや、アドレス信号ADD, およびデータ信号DATAを入力する、あるいは、出力する端子が設けられている。

【0007】

チップ501には、さらに、ロジック特有の制御ピンCTR0, CTR1や、ロジックにアクセス要求をするリクエスト信号REQを入力する端子およびロジックが処理完了を外部に知らせるためのストローブ信号STRBを出力するための端子を含んでいる。

【0008】

【発明が解決しようとする課題】

従来は、ロジック508を制御するために、ロジック508のための特有なピンを設けていたため、図53で示したような汎用的なDRAMに対してピン数が増えたり、またボード上でシステムを組むためにロジック混在DRAMを制御するために専用のコントローラを準備する必要があった。したがって、通常のマイクロコンピュータに接続するような汎用性が失われたり、またはシステムをコン

・ トロールするためにマイクロコンピュータに特殊なコマンドを使う必要があった

【 0 0 0 9 】

この発明の目的は、汎用的な D R A M と同様な制御方法でロジック部を制御することが可能なロジック回路を混載した半導体記憶装置を提供することである。

【 0 0 1 0 】

【課題を解決するための手段】

請求項 1 に記載の半導体記憶装置は、外部から与えられる制御信号、アドレスおよびデータを受ける端子群と、アドレスによって指定される領域に対して制御信号に応じてデータの授受を行なうメモリセルアレイと、メモリセルアレイに対して制御信号、アドレスおよびデータが与えられるシーケンスと同じシーケンスで端子群に制御信号、アドレスおよびデータが与えられた場合に、アドレスが所定の第 1 の領域を指定したときに制御信号、アドレスおよびデータの少なくともいずれか 1 つに応じてデータ処理を行なうロジック回路とを備える。

【 0 0 1 1 】

請求項 2 に記載の半導体記憶装置は、請求項 1 に記載の半導体記憶装置の構成に加えて、端子群から制御信号、アドレスおよびデータを受け、アドレスに応じてメモリセルアレイとロジック回路のいずれか一方に対して、制御信号、アドレスおよびデータの少なくともいずれか 1 つに応じた動作を指示するインターフェイス部をさらに備え、ロジック回路は、インターフェイス部からの指示内容を保持するデータ保持部と、データ保持部の保持内容に応じてデータ処理を行なうデータ処理回路とを含む。

【 0 0 1 2 】

請求項 3 に記載の半導体記憶装置は、請求項 2 に記載の半導体記憶装置の構成に加えて、指示内容は、データ処理回路の動作を指定するコマンドと、データ処理回路が処理する入力データとを含み、データ保持部は、コマンドを保持する第 1 の保持回路と、入力データを保持する第 2 の保持回路と、入力データをデータ処理回路がデータ処理した処理結果を保持する第 3 の保持回路とを含む。

【 0 0 1 3 】

請求項 4 に記載の半導体記憶装置は、請求項 3 に記載の半導体記憶装置の構成に加えて、データ保持部は、データ処理回路がデータ処理を完了したか否かを示すフラグを保持する第 4 の保持回路をさらに含む。

【 0 0 1 4 】

請求項 5 に記載の半導体記憶装置は、請求項 3 に記載の半導体記憶装置の構成において、データ処理回路は、暗号処理を行ない、入力データは、暗号の鍵データを含む。

【 0 0 1 5 】

請求項 6 に記載の半導体記憶装置は、請求項 2 に記載の半導体記憶装置の構成において、指示内容は、データ処理回路の複数の動作モードの指定を含み、データ保持部は、複数の動作モードを保持する保持回路を有し、保持回路は、メモリアレイに一回に書込むデータ幅分のビットの容量を有し、ロジック回路に対する複数の動作モードの指定は、メモリセルアレイに対する 1 回のデータ書込を行なうシーケンスと同じシーケンスで行なわれる。

【 0 0 1 6 】

請求項 7 に記載の半導体記憶装置は、請求項 2 に記載の半導体記憶装置の構成に加えて、インターフェイス部は、制御信号に応じて書換え可能なモードレジスタを含み、インターフェイス部は、モードレジスタの保持値に応じて第 1 の領域をアドレス空間のどこに割当ててゐるかを決定する。

【 0 0 1 7 】

請求項 8 に記載の半導体記憶装置は、請求項 1 に記載の半導体記憶装置の構成において、所定の第 1 の領域は、メモリセルアレイのアドレス空間の一部の領域である。

【 0 0 1 8 】

請求項 9 に記載の半導体記憶装置は、請求項 1 に記載の半導体記憶装置の構成において、所定の第 1 の領域は、メモリセルアレイのアドレス空間以外の仮想的なアドレス空間の一部の領域である。

【 0 0 1 9 】

請求項 1 0 に記載の半導体記憶装置は、請求項 9 に記載の半導体記憶装置の構

成において、ロジック回路は、仮想的なアドレス空間の一部である所定の第1の領域へのアクセスに応じて、所定の第1の領域に対応するメモリセルアレイのアドレス空間に格納されたデータに処理を加える。

【0020】

請求項11に記載の半導体記憶装置の制御方法は、外部から与えられる制御信号、アドレスおよびデータを受ける端子群と、アドレスによって指定される領域に対して制御信号に応じてデータの授受を行なうメモリセルアレイと、メモリセルアレイに対して制御信号、アドレスおよびデータが与えられるシーケンスと同じシーケンスで端子群に制御信号、アドレスおよびデータが与えられた場合に、アドレスが所定の第1の領域を指定したときに制御信号、アドレスおよびデータの少なくともいずれか1つに応じてデータ処理を行なうロジック回路とを備える半導体記憶装置の制御方法であって、第1の領域を予約領域に指定するステップと、メモリセルアレイへの書込シーケンスと同じシーケンスでアドレスによって第1の領域を指定してロジック回路へのコマンドを与えるステップとを備える。

【0021】

請求項12に記載の半導体記憶装置の制御方法は、請求項11に記載の半導体記憶装置の制御方法の構成に加えて、メモリセルアレイへの読出シーケンスと同じシーケンスで第1の領域を指定してロジック回路の処理結果を読出すステップをさらに備える。

【0022】

請求項13に記載の半導体記憶装置の制御方法は、請求項11に記載の半導体記憶装置の制御方法の構成に加えて、半導体記憶装置は、端子群を介して、キャッシュメモリを内蔵するマイクロコンピュータと接続され、第1の領域をキャッシュメモリを使用しない領域として指定するステップをさらに備える。

【0023】

請求項14に記載の半導体記憶装置は、外部から与えられる制御信号、アドレスおよびデータを受ける第1の端子群と、行列状に配置される複数のメモリセルを含み、外部から与えられる選択信号に応じて活性化され、アドレスによって指定される領域に対して制御信号に応じてデータの授受を行なうメモリと、選択信

号に応じてメモリと相補的に活性化され、アドレスおよびデータの少なくともいずれか1つに応じてデータ処理を行なうロジック回路と、選択信号を受ける第2の端子とを備える。

【0024】

請求項15に記載の半導体記憶装置は、請求項14に記載の半導体記憶装置の構成において、メモリは、第1の端子群に時分割に与えられる行アドレスと列アドレスとを含むアドレスに応じてメモリセルの選択動作を行ない、ロジック回路は、第1の端子群に一括して与えられるアドレスに応じて動作を行なう。

【0025】

請求項16に記載の半導体記憶装置は、請求項15に記載の半導体記憶装置の構成に加えて、ロジック回路は、行アドレスと列アドレスの変化を検知して動作タイミングを発生するATD回路を含む。

【0026】

【発明の実施の形態】

以下において、本発明の実施の形態について図面を参照して詳しく説明する。
なお、図中同一符号は同一または相当部分を示す。

【0027】

【実施の形態1】

図1は、本発明の実施の形態1の半導体記憶装置1の構成を示したブロック図である。

【0028】

図1を参照して、半導体記憶装置1は、制御信号／RAS、／CAS、…、／CS、／WEなどの制御信号を受ける端子とアドレス信号ADDを受ける端子とデータ信号DATAを受ける端子と、制御信号／RAS、／CAS、…、／CS、／WE、アドレス信号ADD、およびデータ信号DATAに応じて内部に制御信号を出力するインターフェイス部2と、インターフェイス部2の出力を受けて動作をするDRAM4と、インターフェイス部2から与えられるデータやコマンドとを保持するレジスタ6と、レジスタ6およびインターフェイス部2からの出力に応じて信号処理などの動作を行なうロジック回路8とを含む。

【 0 0 2 9 】

チップ 1 の端子は、汎用 D R A M で用いられている端子のみである。したがって、汎用 D R A M チップを収めているのと同じパッケージを用いることができる。たとえば図 5 3 に示したようなピン配置を有するパッケージである。

【 0 0 3 0 】

そのため、本発明の半導体記憶装置 1 を既存のアプリケーションで用いる場合に、既存の汎用 D R A M と入換えるだけであるので、ボードの再設計や専用の制御 L S I を開発する必要がない。すなわち、汎用 D R A M とピンコンパチブルであるため、ソフトウェアの変更だけで、新たな機能を追加することができる。たとえば新たな機能としては、画像の高速処理用の回路や、暗号処理などのマイクロコンピュータでは時間がかかってしまう処理を行なうロジック回路の追加が考えられる。また、汎用 D R A M を収めているパッケージに数本の未使用の端子、たとえば図 5 3 における 3 6 番ピンや 4 0 番ピンのような N C (ノンコネクション) ピンを用いて制御信号を入力するようにしてもよい。

【 0 0 3 1 】

次に、具体的な制御方法を説明する。搭載されるロジック回路の制御には、いわゆるメモリマップド I O 方式を適用する。

【 0 0 3 2 】

図 2 は、実施の形態 1 のロジック内蔵半導体記憶装置のメモリマップの例を示した図である。

【 0 0 3 3 】

図 2 を参照して、チップに搭載される D R A M の容量を 6 4 M b i t とし、ワード構成を $\times 1 6$ とする。D R A M のアドレスは、X アドレスが X 0 ~ X 1 3 , Y アドレスが Y 0 ~ Y 7 である。よって、8 M B y t e を制御するメモリアドレスは 0 h ~ 3 F F F F F h である。

【 0 0 3 4 】

汎用の D R A M では、このアドレス空間すべてにデータをライトしてリードできる。このようなデータをライトしてリードできる空間を D R A M 空間と呼ぶことにする。本発明では、ある特定の領域を搭載するロジック回路のためのロジック

ク制御領域に割当ててゐる。たとえばアドレスの 0 h ~ 1 F h の空間をロジック制御領域に割当ててゐる。ロジック制御領域の容量は、たとえば、2 5 6 × 2 B y t e の 5 1 2 B y t e である。このアドレス空間に書込むデータによってロジックを制御するコマンドやモードを選択することができる。

【 0 0 3 5 】

図 2 では、最下位アドレスに領域を確保したが、最上位側 (3 F F F F F h ~ 3 F F F E 0 h) にロジック制御領域を割当ててもよい。搭載する D R A M として S D R A M を想定した場合には、モードレジスタセット時にアドレスを割当てて領域を選択することができるようにしてもよい。また、モードレジスタセット時にロジック制御領域を割当てなければ、通常の 6 4 M b i t の S D R A M として使用することもできる。

【 0 0 3 6 】

図 3 は、外部から入力される信号がロジック回路へ伝達される様子を説明するための図である。

【 0 0 3 7 】

図 3 を参照して、インターフェイス部 2 は、制御信号 / R A S , / C A S , … , / C S , / W E 、アドレス信号 A D D 、およびデータ信号 D A T A を受けるバッファ 3 と、バッファ 3 の出力を受けてデコードするデコード回路 5 とを含んでおり、デコード回路 5 の出力に応じてレジスタ 6 はモードやコマンドなどの情報を保持し、これらの保持した情報に応じてロジック回路 8 が制御される。

【 0 0 3 8 】

デコード回路 5 は、アドレス信号 A D D とデータ信号 D A T A をデコードするが、アドレス信号によって指定されるロジック制御領域に書込まれたデータをそのままレジスタ 6 に保存する場合もある。レジスタが、S R A M (スタティックランダムアクセスメモリ) など構成されている場合には、アドレス信号 A D D に応じて指定される S R A M の領域にデータが保持される場合もある。また、レジスタ 6 の代わりに保持回路として D R A M の一部の領域を用い、その領域にロジック回路制御用のデータを保持させてもよい。

【 0 0 3 9 】

図 4 は、実施の形態 1 の半導体記憶装置の標準的なタイミングを説明するための波形図である。

【 0 0 4 0 】

図 4 においては、データ入出力端子から入力および出力が可能な S D R A M において、連続して 8 つのデータを書込みまたは読出す動作を示す。連続して読出されるデータのビット数はバースト長と呼ばれ、S D R A M では通常モードレジスタによって変更することが可能である。

【 0 0 4 1 】

図 4 を参照して、時刻 t_1 において、外部からのクロック信号 $e x t . C L K$ (たとえばシステムクロック) の立上がりエッジで外部からの制御信号 (ロウアドレスストロブ信号 / R A S、コラムアドレスストロブ信号 / C A S、アドレス信号 A D D など) が取込まれる。ロウアドレスストロブ信号 / R A S が活性状態の L レベルにあり、コラムアドレスストロブ信号 / C A S およびライトイネーブル信号 / W E は H レベルにあるため、ロウアクティブコマンド A C T が入力されたことになる。このときのアドレス信号 A D D はロウアドレス $X a$ として取込まれる。

【 0 0 4 2 】

時刻 t_2 において、コラムアドレスストロブ信号 / C A S が活性状態の L レベルとなり、クロック信号 $e x t . C L K$ の立上がり同期して内部に取込まれる。コラムアドレスストロブ信号 / C A S が L レベルで、ロウアドレスストロブ信号 / R A S およびライトイネーブル信号 / W E が H レベルという制御信号の組み合わせは、リードコマンド R E A D である。このときのアドレス信号 A D D はコラムアドレス Y として取込まれる。

【 0 0 4 3 】

アドレスで指定された領域が、図 2 の D R A M 空間である場合には、この取込まれたロウアドレス $X a$ およびコラムアドレス $Y b$ に従って図 1 の D R A M 4 内において行および列の選択動作が実施される。

【 0 0 4 4 】

ロウアドレス $X a$ およびコラムアドレス $Y b$ が図 2 のロジック指定領域のアド

レスである場合には、選択されるのは、図 1 の D R A M 4 の行および列ではなく、レジスタ 6 の所定の領域である。たとえば、この所定の領域には、ロジック 8 の動作状態を示すフラグや、ロジック 8 の演算結果が格納されている。

【 0 0 4 5 】

D/Q は、データ入出力端子から入出力されるデータ信号 D A T A を示す。ロウアドレスストローブ信号/R A S が L レベルに立下がってから所定のクロック周期（図 4 においては 6 クロックサイクル）が経過した後時刻 t 3 において最初のデータ q 0 が出力され、データ q 0 に引き続きデータ q 1 ~ q 7 が連続して出力される。このデータの出力はクロック信号 e x t . C L K の立下がりに対応して出力される。

【 0 0 4 6 】

この出力されたデータは、D R A M 4 に保持されていたデータ、または、レジスタ 6 の内容である。レジスタ 6 の内容は、たとえば、ロジック 8 の動作状態を示すフラグや、ロジック 8 の演算結果である。

【 0 0 4 7 】

時刻 t 4 以降は書込動作を示す。時刻 t 4 において、ロウアクティブコマンド A C T が入力され、ロウアドレス X c が取込まれる。時刻 t 5 において、コラムアドレスストローブ信号/C A S およびライトイネーブル信号/W E がともに活性状態の L レベルであり、かつ、ロウアドレスストローブ信号/R A S が H レベルの組合せ、すなわち、ライトコマンド W R I T E が与えられると、そのときのクロック信号 e x t . C L K の立上がりエッジにおいてコラムアドレス Y d が取込まれるとともに、そのときに与えられていたデータ d 0 が最初の書込データとして取込まれる。

【 0 0 4 8 】

アドレスで指定された領域が、図 2 の D R A M 空間である場合には、ロウアドレスストローブ信号/R A S およびコラムアドレスストローブ信号/C A S の立下がりに対応して、S D R A M 内部においては行および列選択動作が実施される。以降クロック信号 e x t . C L K に同期して順次入力データ d 1 ~ d 7 が取込まれ、対応するメモリセルに書込まれる。

【 0 0 4 9 】

ロウアドレス X c およびコラムアドレス Y d で指定される領域が、図 2 のロジック指定領域である場合には、選択されるのは、図 1 の D R A M 4 の行および列ではなく、レジスタ 6 の所定の領域である。この場合は、入力データ d 1 ~ d 7 は、レジスタ 6 の所定の領域に書込むデータである。たとえば、与えるデータは、ロジック 8 が処理する画像データ、暗号データ等の処理データや、リセット、処理開始等の動作を指定するコマンドデータである。

【 0 0 5 0 】

〔実施の形態 1 の変形例〕

図 5 は、実施の形態 1 の変形例であるロジック内蔵 D R A M 1 0 の構成を示すブロック図である。

【 0 0 5 1 】

図 5 を参照して、ロジック内蔵 D R A M 1 0 は、制御信号 / R A S , / C A S , … , / C S 、アドレス信号 A D D 、データ信号 D A T A を受けるインターフェイス 1 2 と、インターフェイス部 1 2 の出力に応じて動作する D R A M 4 と、インターフェイス部 1 2 の出力に応じて制御用データを保持するレジスタ 1 4 , 1 6 と、レジスタ 1 4 , 1 6 にそれぞれ保持される制御用データに応じて動作するロジック回路 1 8 , 2 0 を有する。

【 0 0 5 2 】

図 6 は、図 5 に示したロジック内蔵 D R A M 1 0 のメモリマップを示した図である。

【 0 0 5 3 】

図 6 を参照して 6 4 M b a t のアドレス空間 0 h ~ 3 F F F F F h のうちアドレス 0 h ~ 1 F h はロジック回路 1 8 に対する制御コマンドやデータを書込むロジック制御領域であり、アドレス 2 0 h ~ 2 F h は、ロジック回路 2 0 に対するコマンドやデータを書込むロジック制御領域である。

【 0 0 5 4 】

このように、メモリマップド I O 空間を、複数個に分割し、搭載する複数個のロジック回路を制御することが可能となる。

【0055】

「実施の形態2」

図7は、実施の形態2のロジック内蔵DRAM30の構成を示すブロック図である。

【0056】

図7を参照して、ロジック内蔵DRAM30は、SDRAM部32と、ロジック部34とを含む。

【0057】

SDRAM部32は、外部からの信号を受けてそれに応じた制御信号を出力するインターフェイス部36と、インターフェイス部36からの出力に応じてデータの保持を行なうDRAMコア38とを含む。インターフェイス部36は、制御信号／CS、／RAS、／CAS、／WEおよびDQMを受ける制御信号入力回路40と、クロック信号CLKおよびクロックイネーブル信号CKEを受けて内部クロックを発生するクロックバッファ44と、クロックバッファ44の出力に同期してアドレス信号A0～Anを取込むアドレスバッファ46と、内部クロックに同期してデータ信号DQ0～DQnの入出力を行なう入出力回路52とを含む。

【0058】

インターフェイス部36は、さらに、制御信号入力回路40の出力に応じコマンド信号ACT、PREなどを出力する制御回路42と、制御回路42の出力に応じてアドレスバッファ46の出力をXアドレス、Yアドレスとしてマルチプレクスするマルチプレクサ48とを含む。

【0059】

マルチプレクサ48は、モードレジスタセット(MRS)コマンドに応じてアドレス信号A0～Amのいずれかの信号ビットに応じて設定可能なモードレジスタ50を含んでいる。

【0060】

DRAMコア38は、行列状にメモリセルが配置されるメモリセルアレイ54と、マルチプレクサ48から与えられるロウアドレスに応じてメモリセルアレイ

54 の行選択を行なうロウデコーダ56と、マルチプレクサ48から与えられるコラムアドレスに応じてメモリセルアレイ54の列選択を行なうロウデコーダ56と、選択されたメモリセルからデータを読み出し、かつ、選択されたメモリセルに対してデータの書込みを行なうセンスアンプドライバ&ライトドライバ60とを含む。

【0061】

ロジック部34は、暗号演算ロジック74と、インターフェイス部36の出力に応じて暗号演算ロジック74の制御をするためのモード情報や暗号演算ロジックに入力するデータおよび暗号演算ロジックの演算結果を保持するレジスタ部72とを含む。

【0062】

レジスタ部72は、アドレス信号A0～Amによって指定される領域が所定値の場合に活性化され、入出力回路52を介して外部から入力されるデータ信号を取込むためのセクタ76と、セクタ76を介して外部から与えられたデータを書込む制御レジスタ78、モードレジスタ80およびデータレジスタ84と、暗号演算ロジックから出力されるデータを保持してその保持データをセクタ76、入出力回路52を介して外部にデータ信号DQ0～DQnとして読出すためのステータスレジスタ82、データレジスタ86とを含む。

【0063】

図8は、実施の形態2のロジック内蔵DRAMに適用されるシステムのメモリマップを示した図である。

【0064】

図8を参照して、システムメモリマップ中の外部RAM領域がロジック内蔵DRAMに対応する。ロジック内蔵DRAMは、その領域がロジック制御領域とDRAM領域に分割されており、ロジック制御領域へのアクセスによって内蔵する暗号ロジックを制御する。このロジック制御領域に対応するシステムメモリマップ上の領域はシステム予約領域とし、CPUのキャッシュおよびMMU（メモリマネジメントユニット）を使用する場合には、キャッシュ不可能領域としておく。また、オペレーティングシステムがこの領域にロードされないように、予め

システムのファームウェアで制御する。さらに、アプリケーションプログラムもこの領域を使用禁止とする。

【0065】

このロジック制御領域は、たとえば、DRAMのロウアドレス $X=3FFFh$ ，コラムアドレス $Y=0H\sim FFh$ に割当ててゐる。

【0066】

図7の制御レジスタ78は $X=3FFFh$ ， $Y=00h$ に割当てられる。モードレジスタ80は、 $H=3FFFh$ ， $Y=01h$ に割当てられる。ステータスレジスタ82は、アドレス $X=3FFFh$ ， $Y=02h$ に割当てられる。第1のデータレジスタ84は、アドレス $X=3FFFh$ ， $Y=03h$ に割当てられ、第2のデータレジスタ86は、アドレス $X=3FFFh$ ， $Y=04h$ に割当てられる。

【0067】

この例では、 $X=3FFFh$ のページ($Y=00h\sim FFh$)を制御コマンド領域に割当てている。したがって、図7の構成でACTコマンド入力時に、 $X=3FFFh$ が入力された時点で、レジスタ部72にアクセスできるようにマルチプレクサを制御しておく。さらに、レジスタのイネーブル信号やレジスタを制御しているクロックも動作させておく。このようにすれば、制御コマンドを入力期間中以外でレジスタ部72で消費する電力を抑えることができる。また、 $X=3FFFh$ のページにリード、ライトコマンドが入っても既にレジスタ部72が活性化されているので、レジスタへのアクセスが遅延されることはない。

【0068】

図7の、暗号演算ロジック74は、ネットワーク上のセキュリティ確保のために使われている主要な暗号方式のアクセラレータを内蔵している。この暗号演算ロジック74は、電子認証で用いられる公開鍵方式と認証後のデータ送受信で用いられる秘密鍵暗号方式の機能をサポートしている。暗号専用のロジック回路で処理するので、処理を汎用のCPUで処理するよりも低消費電力で高速に処理を行なうことができ、たとえば電池駆動のシステム等に適している。

【0069】

図 9 は、図 7 の暗号演算ロジック 7 4 がサポートする暗号方式を示した図である。

【 0 0 7 0 】

図 9 を参照して、暗号演算ロジック 7 4 は、公開鍵暗号方式として R S A をサポートし、秘密鍵暗号方式として D E S 方式と T r i p l e - D E S 方式とをサポートする。さらに、秘密鍵暗号方式では、主要なブロック暗号化モードである E C B (Electric Code Book) , C B C (Cipher Block Chaining) , O F B (Output Feed Back) , C F B (Cipher Feed Back) の各モードをサポートしている。暗号演算ロジック 7 4 は、アプリケーションの適合性を高めるため、暗号化においてクリティカルな処理が割当てられており、その他はロジック内蔵 D R A M 3 0 を制御するマイクロコンピュータ側でソフトウェア処理することになる。そして最大の特徴は、汎用の S D R A M とピンコンパチブルで暗号制御が実現できることである。

【 0 0 7 1 】

次に、図 8 に示したロジック制御領域の各レジスタにどのような割当てがされているかを説明する。

【 0 0 7 2 】

図 1 0 ～図 1 8 は、レジスタに割当てられるデータを説明するための図である。

【 0 0 7 3 】

図 7、図 1 0 を参照して、制御レジスタ 7 8 は、Y アドレスが 0 h の D 0 ～D 1 5 の 1 6 ビットが割当てられている。そして、ビット D 0 に 1 を書込むことにより暗号機能がリセットされる。すなわち、暗号演算ロジック 7 4 に所定時間のリセットパルスを与える処理が実行される。また、ビット D 1 が 1 である場合には、暗号演算ロジック 7 4 が暗号処理中であることを示す。したがって、外部から暗号演算ロジックにアクセスする場合には、ビット D 1 に示されるフラグが 0 であることを確認してからアクセスしなければならない。

【 0 0 7 4 】

この制御レジスタ 7 8 は、公開鍵と秘密鍵の両方式共通に用いられる。

次に秘密鍵方式の制御に用いられるいくつかのレジスタの例について説明する。

【0075】

図7、図11を参照して、Y=1hのアドレスに対しては、モードレジスタ80が割当てられており、この16ビットのうちビットD1、D0は、暗号方式選択に使用される。この2つのビットが“01”であれば暗号方式はDESである“10”であれば暗号方式はトリプルDESである。“00”であれば暗号方式はホールドされる。

【0076】

ビットD5～D2は、ブロック暗号化モード選択に使用される。このビットが“0001”であればブロック暗号化モードはECBが指定される。また“0010”の場合はブロック暗号化モードはCBCが指定される。“0100”の場合には暗号モードはOFBが指定される。これらのビットが“1000”の場合にはブロック暗号化モードはCFB64に指定される。またこれらのビットが“0000”の場合はブロック暗号化モードはホールドされる。

【0077】

ビットD8～D6は暗号処理の単位量を指定するデータ処理モードの選択に使用される。これらのビットが“001”の場合には処理を8Byte単位で行なうノーマルモードが指定され、“010”の場合はブロック長を指定したブロック単位で処理を行なうブロックモードが指定され、“100”の場合にはバッファに蓄積した情報を単位として一括処理するバッファモードが指定され、“000”の場合にはデータ処理モードはホールドされる。

【0078】

このように、Y=1hの1アドレス2Byteのデータの16ビットを複数のモード指定に割当てることができるので、2の16乗の組合せを有効に使用すれば、指定するモードが複数ある場合であっても1回のアクセスで動作モードの指定を完了することができる。

【0079】

図7、図12を参照して、アドレスY=02hにはステータスレジスタ82が

割当てられている。ステータスレジスタのビットD1, D0が“01”であるときは暗号化を示し、“10”であるときは復号化を示し、“00”であるときはホールドを示す。ビットD5, D4が“01”であるときには、平文または暗号文の入力スタートを示しており、“10”であるときには入力ストップを示し、“00”であるときはホールドを示す。

【0080】

ビットD9～D6は、OFB, CFBの1ブロック中のテキスト長を表わす。

図7、図13を参照して、Yアドレス3h～6hは64ビットのDESの鍵などが格納される領域である。

【0081】

図7、図14を参照して、第1のデータレジスタ86は、Triple-DESに使用される鍵を格納する領域である。アドレスY=7h～Ahの領域が相当する。

【0082】

データレジスタ84, 86は、ともに外部からは1本のレジスタに見えるが、実際には複数のレジスタで構成されており、一種のファーストインファーストアウト(FIFO)メモリである。

【0083】

その他には、図7には図示されていないが図15に示すような初期ベクトルを設定するレジスタ、図16に示すようなブロック長の指定をするレジスタ、図17に示すようなバッファ本数を指定するレジスタ、図18に示すようなバッファIDを示すようなレジスタなどがある。

【0084】

なお、公開鍵方式、たとえばRSA暗号処理を行なうために、Y=12h～1Fhの領域は予約領域とされている。公開鍵方式の場合には、暗号処理結果が内蔵のレジスタに保持されるため、暗号処理中であってもDRAM領域にアクセスすることができる。

【0085】

SDRAMに対するACTコマンドで読込まれるロウアドレスXが3FFFh

の場合に、マルチプレクサ 4 8 がこれを検出しセクタ 7 6 を活性化する。そして、リードコマンドまたはライトコマンドでコラムアドレス Y が入力されることによりいずれのレジスタにアクセスするかが選択される。そして入出力回路 5 2 を介して外部から入力されるデータがレジスタに書込まれる。

【 0 0 8 6 】

実施の形態 2 の場合には、ロジック制御領域として確保したアドレス領域は、3 F F F 0 0 h ~ 3 F F F F F h であったが、モードレジスタセット命令でセットできる図 7 におけるレジスタ 5 0 の保持内容に応じて、マルチプレクサにおいて割当てアドレスを変更できるようにすることにより、さまざまなマイクロコンピュータシステムに本発明のロジック内蔵 D R A M を搭載することが可能となる。モードレジスタセット命令でアドレスを割当てない場合には、本発明のロジック内蔵 D R A M は通常の 6 4 M b i t の S D R A M として使用可能である。通常の S D R A M として使用する用途のために、モードレジスタに内部搭載ロジックを使用するか否かを指定するビットを設けてもよい。

【 0 0 8 7 】

〔実施の形態 3〕

図 1 9 は、本発明のロジック内蔵 D R A M 9 2 とマイクロコンピュータ 9 0 とが接続される様子を示した図である。

【 0 0 8 8 】

マイクロコンピュータ 9 0 には、CPU コア 9 4 と、キャッシュメモリ 9 6 と、メモリコントローラ 9 8 および外部バスインターフェイス回路 1 0 0 が含まれており、これらは内部バス 1 0 2 によって接続されている。外部バスインターフェイス回路 1 0 0 は、CPU コア 9 4 からの指令に応じてロジック内蔵 D R A M に対して制御信号およびアドレス信号およびデータを出力する。したがって、外部バスインターフェイス回路 1 0 0 とロジック内蔵 D R A M 9 2 とは制御信号 / R A S , / C A S , … , / C S などの制御信号を伝達する制御信号バスと、アドレス信号 A D D . を伝達するアドレスバスとデータ D A T A を伝達するデータバスとによって接続されている。

【 0 0 8 9 】

このようなシステムにおいてロジック内蔵DRAM92を制御するためには、マイクロコンピュータ90上で走るソフトウェアで留意しなければならない事項がある。

【0090】

図20は、ロジック内蔵DRAMの制御を説明するためのフローチャートである。

【0091】

図20を参照して、まず最初にステップS1において、ロジック制御領域となるアドレスを予約領域に指定する。つまり、ロジック回路に対するコマンド制御用のアドレス空間上にプログラムが割当てられないようにする。割当てない方法としては、たとえば、OS（オペレーションシステム）の機能を用いてロジック制御領域を予約領域にする方法がある。

【0092】

メモリー管理、割り込み管理、プロセス間通信といったシステムの基本的な制御を行う、OSにおける中核部分であるカーネル自体がロジック制御領域に割当てられないように、OSの立上がり時点にも注意を要する。したがって、カーネル自体がロジック制御領域に割当てられないように注意して、予約領域をOS側で指定しておく。

【0093】

次に、ステップS2において、データキャッシュありのシステムにおいては、ロジック制御領域をキャッシュ不可能領域にしている。

【0094】

すなわち、図19におけるCPUコア94からロジック内蔵DRAM92に対して所定のアドレス空間を指定してコマンドに相当するデータを内部バス102に送った場合であっても、キャッシュメモリ96が動作すると、そのコマンドに相当するデータはキャッシュメモリ96に書込まれてしまい、ロジック内蔵DRAM92には伝達されない場合があり得る。すると、ロジック内蔵DRAM92に搭載しているロジック回路は、そのコマンドに応じて動作できなくなる。したがって、ロジック制御領域がキャッシュされないように設定する必要がある。大

抵のマイクロコンピュータでは、一部のアドレス空間をアンキャッシュابل領域に指定する制御が可能である。

【0095】

また、メモリマネージメントユニット機能を有している場合には、仮想アドレス空間がロジック制御領域で用いられないように設定する。

【0096】

このように、キャッシュメモリがあるようなシステムでは、システムの初期設定において、ロジック内蔵DRAMのロジック制御領域に対しては、キャッシュメモリを使用しないようにし、必ずアクセスされるようにする。

【0097】

次に、ステップS3において、割当てた領域にノーマルライトすることによってロジック制御のためのコマンドを入力し、ステップS4においてノーマルリードによりロジックの処理状況のチェックや処理結果の読出を行なうことができる。さらに、ステップS5において処理がまだ終了していなければ、ステップS3、S4を繰返すことになる。具体的には、図10で説明したように、アドレスY=0hのビットD1に書込まれているフラグをチェックすることにより、処理状況を判断することができる。このフラグをチェックして、処理の完了を確認してからマイクロコンピュータは演算結果をアクセスするなど次の動作を始めることができる。

【0098】

したがって、本発明によれば、従来では処理の終了を専用のピンで受け手側に伝えていたのに対しSDRAMに通常のノーマルリードを行なうことによりフラグ状態をチェックすることが可能となる。

【0099】

〔実施の形態4〕

実施の形態1～実施の形態3で示した例は、チップに搭載するDRAMメモリの一部の空間をつぶしてコマンド制御用の空間を割当てていた。したがって、割当てた部分だけはマイクロコンピュータシステムのメインメモリとしては使えなかった。

【0 1 0 0】

実施の形態4では、ゴースト空間を制御用に割当ててゐる。

図21は、実施の形態4において割当てたメモリマップを示した図である。

【0 1 0 1】

図21を参照して、搭載するDRAMを、64Mbitの容量でワード構成が×16のSDRAMであるとする、XアドレスはX0～X13、YアドレスはY0～Y7であった。Xアドレスを1端子追加し、X14 = “0”の領域を実メモリ空間とし、X14 = “1”の領域をゴースト空間とする。メモリが存在しないこのダミーのゴースト空間の一部をロジック制御領域に割当ててゐる。この空間には必ず直接アクセスがされるように実施の形態3で示したような工夫をしておく。

【0 1 0 2】

X14を与えるための端子が1端子増加することになるが、パッケージで未使用端子がある場合にはそれを割当てればよい。たとえば図53の40番ピンや36番ピンなどのNC端子を割当てればよい。図21ではX14のアドレスを追加した場合を示したが、Yアドレスを1ビット追加してもよい。すなわちY8 = 0の領域をDRAM空間とし、Y8 = 1の領域をゴースト空間とすることもできる。DRAMではXアドレスとYアドレスとは、通常はマルチプレクスされており、Xアドレスのほうがビットが多いので、Yアドレスを追加する場合には、使用する端子の追加は必要ない。

【0 1 0 3】

以上は、ゴースト空間の一部にロジック制御領域を割当てた場合を示したが、ゴースト空間に対してリードすると、それに対応する実空間のアドレスに格納されているデータに演算が加えられて出力されたり、そのアドレスのデータが書き直される場合も考えられる。すなわち、X14 = 1としてアクセスすると、指定したアドレスのX14 = 0とした実空間のアドレスに保持されているデータに何らかの処理を加えるようにしてもよい。この場合においても、X14のアドレスを拡張する代わりにY8のアドレスを拡張してもよく、また、X14が1の場合にゴースト空間としたが、X14 = 0の場合をゴースト空間とし、X14 = 1の

場合を実メモリ空間としてもよい。Y 8 のアドレスを拡張する場合も Y 8 = 0 の場合をゴースト空間とし、Y 8 = 1 の場合を実メモリ空間としてもよい。

【 0 1 0 4 】

〔実施の形態 5〕

図 2 2 は、実施の形態 5 のロジック内蔵 DRAM 1 1 1 の構成を示した図である。

【 0 1 0 5 】

図 2 2 を参照して、ロジック内蔵 DRAM 1 1 1 には、通常の DRAM 1 1 4 を制御するためのアドレス ADD、データ DQ およびクロック信号 CLK や制御信号 /RAS、/CAS、…、/CS、/WE を制御するための端子に加えて、信号 WE__L、ADD__L を与えるための端子が設けられている。

【 0 1 0 6 】

ロジック内蔵 DRAM 1 1 1 は、さらに、通常の DRAM 1 1 4 と、所定の制御信号を保持するためのレジスタ 1 1 6 と、レジスタ 1 1 6 の保持情報に応じて動作するロジック回路 1 1 8 とを含む。

【 0 1 0 7 】

すなわち、制御専用の端子を最小限付け加えることによって制御空間を自由に設定することができる。図 2 2 では、追加した制御端子は、制御信号 WE__L、ADD__L が入力される端子である。追加する端子は、図 5 3 で示した 3 6 ピンや 4 0 ピンのような NC ピンに割当てればよい。

【 0 1 0 8 】

制御信号 ADD__L が L レベルの場合に DRAM アクセスモードにされ、制御信号 ADD__L が L レベルから H レベルになると、DRAM 1 1 4 は非活性化され代わりにレジスタ 1 1 6 に信号が入力可能となりロジック 1 1 8 が動作するモードとなる。

【 0 1 0 9 】

図 2 3 は、実施の形態 5 におけるマイクロコンピュータシステムのメモリマップを示した図である。

【 0 1 1 0 】

図 2 3 を参照して、0 h ~ 3 F F F F F h が D R A M 空間に割当てられる。X アドレスが X 0 ~ X 1 3 の 1 4 ビット、Y アドレスが Y 0 ~ Y 7 の 8 ビットであり、マイクロコンピュータシステムにおいて D R A M 空間を指定するアドレスビットとしては、あわせて A 0 ~ A 2 1 までは用いられる。

【 0 1 1 1 】

そして、たとえば、制御信号 A D D _ L が入力される端子をマイクロコンピュータシステムのアドレスビット A 2 3 と接続した場合には、ロジック制御領域は、8 0 0 0 0 0 h ~ 8 0 3 F F F h を割当てることができる。つまり、アドレスビット A 2 3 = “1” とし、アドレスピンマルチプレクスを使用しないときに、アドレスを入力する最大数の端子から D R A M のアドレスとして指定することができる範囲すなわち、X アドレスとして指定可能な範囲と同じ 0 h ~ 3 F F F h がロジック制御領域として割当て可能な範囲である。実際に使用する際には、ロジック制御領域の上限は必要に応じて設定すればよい。

【 0 1 1 2 】

ただし、マイクロコンピュータが、アドレスビット A 2 3 = “1” である他のアドレス領域を使用する可能性がある場合には、ロジック制御領域（8 0 0 0 0 0 h ~ 8 0 3 F F F h）にアクセスする場合のみ、ロジック内蔵 D R A M に対してチップセレクト信号 / C S を活性化させる必要がある。

【 0 1 1 3 】

図 2 4 は、実施の形態 5 のロジック内蔵 D R A M の制御を説明するための動作波形図である。

【 0 1 1 4 】

図 2 4 を参照して、時刻 t 1 まではクロック信号 C L K に同期した通常の D R A M に対するアクセスが行なわれる。

【 0 1 1 5 】

時刻 t 1 において制御信号 A D D _ L が H レベルになると、ロジック回路に対するコマンド制御モードに入る。以降、クロック信号 C L K に同期してアドレス信号 A D D によって指定されたレジスタにデータの授受が行なわれる。図 2 4 の場合には、追加された制御信号 / W E _ L が L レベルであるので、コマンド制御

用レジスタにコマンド入力となされる。

【0116】

〔実施の形態5の変形例〕

図25は、実施の形態5の変形例を説明するための図である。

【0117】

通常のDRAMアドレス空間をアクセスするときには、マイクロコンピュータ132は、CPUコア134から指定されたアドレスに対して、メモリコントローラ136がマルチプレクス回路140を用いてXアドレスおよびYアドレスをアドレス信号A0～A13が伝達されるアドレスバスにマルチプレクスして出力する。

【0118】

しかし、図23で示したように、DRAM空間とは異なる領域にロジック制御領域が割当てられる場合には、メモリコントローラ136は、マルチプレクス回路140を用いなくてそのままアドレスを外部バスインターフェイス回路142から出力することになる。

【0119】

この場合には、アドレス信号A0～A20のうち、マルチプレクスされた後有効となっているピン数に対応するアドレス信号A0～A13を用いてSRAMと同様な方法でアドレスの指定となされる。この場合、信号A14～A20は何であってかまわない状態、いわゆる「Don't Care」の状態である。このようなアドレス信号A0～A20が／CSの活性化とともに指定されると、応じてロジック内蔵DRAM121が処理を行なう。

【0120】

ただし、この場合も、マイクロコンピュータが、アドレスビットA23＝“1”である他のアドレス領域を使用する可能性がある場合には、ロジック制御領域（800000h～803FFFh）にアクセスする場合のみ、ロジック内蔵DRAMに対してチップセレクト信号／CSを活性化させる必要がある。

【0121】

かかる場合には、ロジック内蔵DRAM121は、レジスタ126の一部にア

ドレスの変化を検知するA T D (Address Transition Detect) 回路 1 3 0 を設ける。

【 0 1 2 2 】

図 2 6 は、実施の形態 5 の変形例の動作を説明するための動作波形図である。

この場合には、時刻 t_1 までは、制御信号 ADD_L は L レベルであり、通常の DRAM アクセスがなされるが、 ADD_L が H レベルになると、ロジック回路に対するコマンド制御モードに入る。このとき、 $/WE_L$ が H レベルの場合には、ライトモードが指定されて $/WE_L$ が H レベルの場合にはリードモードが指定される。

【 0 1 2 3 】

そして、アドレス信号 $A_0 \sim A_{13}$ によって指定されるアドレス ADD が変化すると、A T D 回路 1 3 0 がこれを検知し、クロック信号 CLK にかかわらず内部の動作クロックを発生し DQ に与えられる信号を内部のコマンドレジスタにライトしたり、アドレスで指定されるレジスタの内容を DQ 端子からリードすることができる。

【 0 1 2 4 】

以上説明したように、半導体記憶装置 1 2 1 の制御信号 $/WE_L$ を受ける端子とマイクロコンピュータ 1 3 2 側の S R A M 制御用に出力される信号 A_{23} が出力される端子とを接続することで、半導体記憶装置 1 2 1 を S R A M のように制御すれば特殊な機能をマイクロコンピュータ側に入れる必要がない。マイクロコンピュータは、外部拡張した S R A M 等のメモリに対してデータの書込または読出を行なう通常のコマンドを実行すれば、半導体記憶装置 1 2 1 に搭載したロジック回路を制御することができる。

【 0 1 2 5 】

〔実施の形態 6〕

実施の形態 6 では、より具体的な暗号ロジック内蔵 DRAM について説明する。以降、この暗号ロジック内蔵 DRAM をセキュリティー S D R A M (S c R A M) と称する。

【 0 1 2 6 】

図 2 7 は、S c R A M 2 0 0 の構成を示したブロック図である。

図 2 7 を参照して、S c R A M 2 0 0 は、外部からクロック信号 C L K を受けるクロックバッファ 2 0 2 と、外部とデータ信号 D Q を授受するための入出力バッファ 2 0 4 と、外部からアドレス信号 A D D 、コマンド信号 C M D および信号 C R Y P を受ける入力バッファ 2 0 6 とを含む。

【 0 1 2 7 】

S c R A M 2 0 0 は、さらに、入力バッファ 2 0 6 の出力に応じて動作モード情報を保持するモードレジスタ 2 0 8 と、入力バッファ 2 0 6 およびモードレジスタ 2 0 8 の出力に応じて S c R A M の制御を行なう D R A M 制御アドレスカウンタ 2 1 0 と、D R A M 制御アドレスカウンタ 2 1 0 の制御の下にデータ保持動作を行なう D R A M 部 2 1 2 とを含む。

【 0 1 2 8 】

入出力バッファ 2 0 4 と D R A M 部 2 1 2 とは内部バス m b u s [1 5 : 0] で接続される。D R A M 部 2 1 2 は、複数のバンクを備えており、各バンクはメモリアレイ、ロウデコーダ、コラムデコーダおよびセンスアンプ、入出力制御回路を含んでいる。

【 0 1 2 9 】

S c R A M 2 0 0 は、さらに、セレクタ 2 1 4 と、レジスタ R E G 0 , R E G 1 , R E G 2 と、カウンタ 2 2 0 , 2 2 4 と、制御回路 2 2 2 と、暗号ロジック 2 2 8 とを含む。

【 0 1 3 0 】

モードレジスタ 2 0 8 には、S D R A M の制御コマンドであるモードレジスタセット (M R S) 時のパラメータが保存される。このパラメータとしては、S D R A M のモード設定だけでなく、制御レジスタ R E G 0 ~ R E G 2 のアクセスのイネーブル／ディスエーブルも設定できる。また、M R S が入力されると制御レジスタ R E G 0 ~ R E G 2 および暗号ロジック 2 2 8 がリセットされる。

【 0 1 3 1 】

S c R A M 2 0 0 には、暗号ロジック機能を制御するために 3 種類の制御レジスタ R E G 0 ~ R E G 3 が設けられている。

【 0 1 3 2 】

制御レジスタ REG 0 は暗号ロジックを制御するコマンドや、モードを制御するためのレジスタである。制御レジスタ REG 1 は、暗号ロジックの入力データの保持をするレジスタである。制御レジスタ REG 1 の保持容量は最大 4 k b である。

【 0 1 3 3 】

制御レジスタ REG 2 は、暗号ロジックの出力結果を保持するレジスタである。制御レジスタ REG 2 もその保持容量は最大 4 k b である。

【 0 1 3 4 】

次に、制御レジスタ REG 0 ～ REG 2 に対するアクセス方法を説明する。

外部から制御レジスタをアクセスすることにより、S c R A M 2 0 0 の内蔵する暗号ロジックの制御、データの入出力、低消費電力化モードの制御を行なうことができる。

【 0 1 3 5 】

図 2 8 は、制御レジスタの設定に応じたメモリマップの状態変化を説明するための図である。

【 0 1 3 6 】

図 2 8 を参照して、S c R A M の内蔵する暗号機能を制御するには、2 通りの方法がある。

【 0 1 3 7 】

まず第 1 の方法は、制御レジスタアクセスイネーブル信号 C R Y P として外部から 1 を入力することである。これにより、X = # 3 F F F のページが制御レジスタ領域となる。

【 0 1 3 8 】

第 2 の方法は、制御レジスタアクセスイネーブル信号 C R Y P が 0 の場合に、S D R A M のモード設定のため M R S コマンドを入力するときに、アドレスビット A 1 0 として 1 を入力することである。この場合は、アドレスビット A 1 1 が 0 の場合には、X = # 3 F F F のページが制御レジスタ領域になる。また、アドレスビット A 1 1 が 1 の場合には、X = # 0 0 0 0 のページが制御レジスタ領域

となる。

【0139】

S c R A M の制御レジスタを使用しない場合は、S D R A M のモードを設定するための通常の M R S コマンドを A 1 0 = . 0 に設定することにより入力する。この場合、制御レジスタアクセスイネーブル信号 C R Y P = 0 にする必要がある。信号 C R Y P や M R S コマンド入力から t R S C 以降には、S c R A M は新たなコマンドに対して動作可能となる。

【0140】

制御レジスタアクセスがイネーブルの期間、特定のロウアドレス (X = # 3 F F F または、 X = # 0) のアドレス空間に、定められたデータをライト／リードすることによって、制御用レジスタ R E G 0 ～ R E G 2 にアクセスすることができる。この間は、暗号をロジック制御用に割当てられた 4 k ビットのアドレス空間をメモリとして用いることはできない。それ以外の空間については、通常のメモリ領域として外部からアクセスすることが可能である。

【0141】

ここで、制御レジスタアクセスに対応するアドレス空間に外部からアクセスした場合には、D R A M 部 2 1 2 に対してはアクセスが行なわれない。したがって、制御レジスタアクセスのイネーブル状態から抜ければ、制御レジスタ領域であった特定のロウアドレスに対応するメモリ空間を通常のメモリ空間としてアクセスすることができる。制御レジスタアクセスのイネーブル状態から抜ける前にレジスタに設定した値は、信号 C R Y P を 0 にして動作モードから抜けた場合には保持される。しかし、M R S コマンドを用いてモードから抜けた場合には、レジスタに設定した値はリセットされる。すなわち、M R S コマンドを入れることにより、レジスタをリセットすることができる。

【0142】

制御用レジスタ R E G 0 ～ R E G 2 に対するアクセスは、制御用レジスタに割当てられたアドレス空間内で、汎用 S D R A M と同じシーケンスでアクセスすることにより行なわれる。制御レジスタからの読出データは、S D R A M のモードレジスタセット時に設定された同じ C A S レイテンシで出力されるが、制御用の

レジスタへのアクセス時のバースト長は1に固定される。

【0143】

次に、図27のモードレジスタ208について説明する。

図29、図30、図31は、図27に示したモードレジスタ208を説明するための図である。

【0144】

図29を参照して、モードレジスタセット命令はクロック信号CLKの立上がり時にコマンド信号CMDに含まれる信号/C S, /R A S, /C A S, /W E をすべてLレベルに設定することにより与えられ、このときにアドレス信号ADDに含まれるアドレスビットBA0, BA1, A0~A11で設定される値が図30に示す各ビットに書込まれる。ただし、アドレスビットA8, A7は、0に設定される。他のビットは図31で示すように種々の設定に割当てられている。

【0145】

モードレジスタセットではSDRAMのモード設定、SDRAMのローパワーモード設定、および制御レジスタのアクセスを行なうことができる。

【0146】

SDRAMのモード設定では、バースト長、バーストタイプ、および/C A S レイテンシをプログラムすることができる。

【0147】

SDRAMのローパワーモード設定では、非パワーダウンモード時のプリチャージスタンバイ電流を低減することができる。ただし、このモードを使用するには、入力信号のセットアップタイムを5 n s 以上にする必要がある。

【0148】

制御レジスタのアクセスでは、モードレジスタセット時に、ビットA10を1にすると、暗号機能を制御するためのレジスタ空間が現われる。この方法は、信号CRYPを入力する端子の制御ができないために、この端子を0に固定したシステムに適している。制御レジスタへのアクセスは、SDRAMのアクセスシーケンスと同じで、同じ/C A S レイテンシでデータが出力される。しかし、制御レジスタのアクセスは常にバースト長が1に固定されている。

【 0 1 4 9 】

モードレジスタセットによりセットされたデータは、次のMRSコマンドが入力されるまでモードレジスタに格納される。次のMRSコマンドは、両バンクが非活性化状態にあれば入力できる。MRSコマンドからtRSC後には、SDRAMは新たなコマンドに対して動作可能となる。また、MRSコマンドが入力されると制御レジスタがリセットされる。制御レジスタの内容を保持したまま、制御レジスタアクセスのディスエーブルとイネーブルとを切換えるには、SDRAMのモードレジスタセット時にビットA10を0にして信号CRYPの制御を行なうことで実現することができる。

【 0 1 5 0 】

図32は、ScRAMの暗号制御エントリ・エグジットに関連する状態遷移図である。

【 0 1 5 1 】

電源投入がされると初期状態340にScRAMの状態が遷移する。続いて信号CRYPを1にすると、暗号制御がイネーブルな状態344に遷移する。一方信号CRYPが0の場合であっても、モードレジスタセットコマンドによりビットA10を1に設定することにより暗号制御イネーブル状態344に遷移させることができる。

【 0 1 5 2 】

パワーオンの初期状態340において信号CRYPを0に設定し、モードレジスタコマンドによってビットA10を0にすると暗号制御ディスエーブルな状態342に遷移する。

【 0 1 5 3 】

状態342から344に遷移させるためには、信号CRYPを1にすることによる場合と、信号CRYPが0の状態であってモードレジスタセットコマンドによりビットA10を1に設定することによる場合とがある。

【 0 1 5 4 】

一方、暗号制御イネーブル状態344から暗号制御ディスエーブル状態342に遷移させるには、暗号制御イネーブル状態344に信号CRYPを1に設定し

て入った場合には逆に信号C R Y Pを0に設定することにより遷移させることができる。また、信号C R Y Pを0に設定し、モードレジスタセットコマンドでビットA 1 0を1に設定してイネーブル状態3 4 4に入った場合には、モードレジスタセットコマンドによりビットA 1 0を0に設定することによりディスエーブル状態3 4 2へと遷移させることができる。

【0155】

図3 3は、制御レジスタアクセスの一例を示した動作波形図である。

図3 3を参照して、制御レジスタアクセス領域としてX=#3 F F Fのページが割当てられた場合を示す。SDRAMのモードがCASレイテンシCL=3に設定されているので、レジスタ出力もCL=3のタイミングになっている。

【0156】

ここで、モードレジスタセットにより設定されたバースト長BLによらず、レジスタアクセスに関しては、バースト長は1に固定される。したがって、リード/ライトコマンドとコラムアドレスとを毎サイクル入力する必要がある。

【0157】

図3 4～図3 7は、制御レジスタのアドレスマップを示した図である。

図3 4はコラムアドレスがh 0 0, h 0 1の場合を示し、図3 5は、コラムアドレスがh 0 2の場合を示し、図3 6は、コラムアドレスがh 0 3, h 0 4, h 0 5, h 0 6の場合を示す。図3 7は、コラムアドレスがh 1 3～h 2 0の場合について示す。

【0158】

これらのXアドレスはX=h 3 F F FまたはX=h 0 いずれかに初期設定された値である。

【0159】

次にS c R A Mの内蔵する暗号機能の特徴について説明する。

S c R A Mは、ネットワーク上のセキュリティ確保のために使われている、主要な暗号方式のアクセラレータを内蔵している。また、S c R A Mは、電子認証で用いられる公開鍵方式と認証後のデータ送受信で用いられる秘密鍵暗号方式の機能をサポートしている。これらは、図2 7に示す専用の暗号ロジック2 2 8で

処理するので、低消費電力で高速暗号処理が必要なシステムに適する。

【0160】

サポートする暗号方式については、図9で示した場合と同様であり、公開鍵暗号方式としてRSAを、秘密鍵暗号方式としてDESとトリプルDESとをサポートしている。さらに、秘密鍵暗号方式では、主要ブロック暗号モードであるECB, CBC, OFB, CFB-64をサポートしている。

【0161】

一般的なネットワークだけでなく、インターネットでも、これらの暗号方式は主要な暗号方式として用いられている。主要なブラウザであるネットスケープコミュニケーターやインターネットエクスプローラなど、暗号化電子メール方式であるS/MIMEにも対応することができる。今後の拡大が期待される電子商取引市場では、これらの暗号方式を用いたセキュリティの確立が重要になると考えられる。また、携帯電話への運用が予想されるワイヤレスアプリケーションプロトコル(WAP)でも上述の暗号化方式がサポートされるため、ScRAMは、さまざまなシステムに幅広い適合性がある。

【0162】

ScRAMは、アプリケーションの適合性を高めるため、内部暗号ロジックにより、暗号化でクリティカルな処理のみを受け持つ。すなわち、ハッシュ、データエンコーディング、パディングなどの処理は、従来どおりソフトウェア側で受け持つことになり、アプリケーション側の自由度を高めるように考慮されている。また、RSAでは、ソフトウェア処理で要する処理時間の大部分を占めていた次のa), b)の演算のみを処理する。

【0163】

a) RSAによる電子認証を高速化するため、

べき乗剰余演算 $M^e \bmod N$ 、

モンゴメリー乗算剰余演算 $X * Y * R^{-1} \bmod N$ 、

剰余演算 $Y \bmod N$

を実施する。

【0164】

b) 暗号化通信の高速化をするために、トリプルDES、DES (CBC, ECB, OFB, CFB-64) の演算を行なう。ただし、最終テキストブロック部のパディング処理は、規格によってさまざまであるので、適宜、ソフトウェアで処理する必要がある。

【0165】

続いて、暗号処理速度について述べる。

アドレス処理専用ロジックとDRAMのワンチップ化によって、高速化と低消費電力化とを実現している。その結果、携帯端末に適した低電源電圧 (2.5V系) で、

1024bit RSA暗号署名処理時間: 100-200ms

約60MbpsのトリプルDES処理。DESであれば、約180Mbps。の性能を実現することができる。

【0166】

また、ScRAMは、特定のアドレス空間をアクセスすることで、暗号ロジック部分を制御しているので、汎用SDRAMとピン交換を実現することができる。また、暗号機能をディスエーブルにすれば、SDRAMとしての機能のみを使用することもできる。

【0167】

続いて暗号機能制御方法について説明する。

先に説明したように、ScRAMに内蔵している暗号機能の制御は、制御レジスタに対してアクセスを行なうことで実行することができる。制御レジスタにアクセスするには、モードレジスタセット時に所定のアドレスを入力するか、信号CRYPが与えられる端子を1に設定して、特定のアドレスにアクセスすることによって制御レジスタにアクセスすることができる。ここで、制御レジスタに割当てられたデフォルトのアドレス空間は、 $X = h3FFF$ のページである。また、MRSコマンド入力時に、ビットA10, A11をともに1に設定すれば、 $X = h0$ のページに制御レジスタを割当てることができる。

【0168】

しかし、ファームウェア設計では、制御レジスタアクセスのために予約された

空間を、それ以外の用途で使わないことが要求される。たとえば、アプリケーションやカーネルにこの空間を割当ててることを禁止しなければならない。カーネルに関しては、ブート時に割当てられないように注意する必要がある。

【0169】

続いて、システム設計の例を説明する。

図38は、信号C R Y Pを与える端子を制御可能なシステムを説明するための図である。

【0170】

図38を参照して、一般のマイコン(MCU)が備えているI/Oポートを、C R Y P信号を受ける端子に接続することができるシステムについて例示している。この構成では、システムのブート前にC R Y P端子を0にすることができれば、制御レジスタに割当てられたアドレス空間が現われていないので、プログラムを初期ロードする空間には制約がない。プログラムがロードされた領域が $X = h3FFF$ を含んでいる場合には、その後C R Y P端子を1に設定して、制御レジスタに割当てられたアドレス空間を $X = h0$ のページに変更する必要がある。

【0171】

図39、図40は、C R Y P端子を制御不可能なシステムについて説明するための図である。

【0172】

図39を参照して、C R Y P端子に与える値を0に固定した場合には、S c R A Mのモードレジスタセット(MRS)入力時に、ビットA10を1にして制御レジスタへのアクセスをイネーブルにする。このときに、ビットA11でプログラムがロードされていない空間を選択する。

【0173】

図40を参照して、C R Y P端子に与える値を1に固定した場合には、 $X = h3FFF$ のページに制御レジスタへのアクセス空間が割当てられるので、この空間を避けてプログラムのロードを行なう必要がある。

【0174】

図41は、制御レジスタへの設定の説明をするための動作波形図である。

図4 1を参照して、制御レジスタの設定に関して信号入力の一例が示される。制御レジスタへのアクセスでDRAMと唯一異なる点は、MRSの設定によらずバースト長が1になることである。それ以外に関しては、DRAMと同じタイミング、かつ、同じシーケンスで、制御レジスタに対してアクセスを行なう。

【0175】

図4 1では、制御レジスタにアクセスするためのアドレス空間が $X = h3FF$ Fの場合を例として示している。

【0176】

まず時刻 t_1 において、制御レジスタにアクセスするためのアドレス $X = h3FF$ F F Fが入力される。

【0177】

続いて時刻 t_2 において、ソフトリセットがされる。

時刻 t_3 では、モード設定(1)がなされる。モード設定(1)は、秘密鍵暗号方式としてDES-56を選択し、CBCモードで処理を行なうモード設定である。

【0178】

続いて時刻 t_4 ではモード設定(2)が行なわれる。モード設定(2)は、暗号化、REG1とREG2のアドレスカウンタをリセット。初期値としてIVを使う。というモードが設定される。

【0179】

時刻 $t_5 \sim t_6$ では、秘密鍵が入力される。

時刻 $t_6 \sim t_7$ では、イニシャルベクトルIVが入力される。

【0180】

時刻 $t_7 \sim t_8$ では、8バイト単位の平文を入力し、平文入力後時刻 t_8 においてEOF(エンドオブファイル)の入力が行なわれる。

【0181】

そして時刻 t_9 では、フラグ領域に対するリードを行ない、暗号ロジックが処理中か否かをチェックする。

【0182】

このチェック結果はC A S レイテンシでデータ信号D Qとして読出される。

続いて、S c R A Mがサポートする秘密鍵暗号方式について説明する。

【0183】

図4 2～図4 4は、暗号化処理の基本単位について示した概略図である。

図4 2は、鍵の長さが56 b i tのD E Sを示し、図4 3は、鍵の長さが112 b i tのトリプルD E S方式を示し、図4 4は、鍵の長さが168 b i tのトリプルD E S方式について示している。S c R A Mでは、秘密鍵暗号化方式としてD E SとトリプルD E Sとをサポートしている。インターネットのセキュリティソケットレイヤ、S/M I M Eの電子メール、ワイヤレスアプリケーションプロトコルでこれらの暗号化方式は利用されている。なお、トリプルD E Sは、D E Sを暗号化－復号化－暗号化の3回処理を行なったものである。

【0184】

図4 5～図4 7は、復号化処理の単位について示した概略図である。

図4 5は、図4 2の暗号化に対応する復号化を示し、図4 6は、図4 3の暗号化に対応する復号化を示し、図4 7は、図4 4の暗号化に対応する復号化を示す。

【0185】

続いて、S c R A Mがサポートする秘密鍵暗号の暗号利用モードについて説明する。例として、E C B、C B Cの2つのモードについて説明する。

【0186】

図4 8、図4 9は、E C Bモードについて説明するための図である。

図4 8、図4 9を参照して、E C Bモードは基本モードであり、暗号／復号処理基本単位に当たる。暗号化では、通常データ（平文）Mを図4 8に示すように64ビットごとに分解したブロックM_i（M=M₁、M₂、M₃…）を送信者と受信者のみが共通に持つ秘密の鍵と呼ばれるデータKを用いて、各ブロックごとに暗号化処理を行なう。そして、64ビットの暗号文C_i（C=C₁、C₂、C₃…）が生成される。復号化では、図4 9に示すように、64ビットの暗号文C_iを受取り、暗号化に用いたものと同じ鍵データKを用いて、平文M_i（M=M₁、M₂、M₃…）を生成する。

【0187】

次にCBCモードについて説明する。

図50は、CBCモードの演算を説明するための図である。

【0188】

図50を参照して、CBCモードでは、まず暗号化は、平文 M を64ビットごとに分解したブロック M_i をECBモードと同様に暗号化を行なう。そして、さらに、この暗号文ブロック C_i と、次のブロック M_{i+1} との排他的論理和を次の暗号化の入力とする。これを繰返して次々と連鎖させるのである。

【0189】

一方、復号化は、暗号ブロック文 C_i をECBモードと同様に復号化した結果を M_i とし、 C_i を次の暗号文ブロック C_{i+1} の復号結果との排他的論理和をとり、出力平文ブロック M_{i+1} とする。これを繰返して次々と連鎖させるのである。なお、図50において、平文は M_i 、暗号文は C_i ($i = 1, 2, \dots$)、暗号鍵 K を用いた暗号化を E_k 、復号化を D_k とする。

【0190】

また、IV（イニシャルベクトル）は初期値であり、最初の暗号化と復号化の際に用いられる。IVは、暗号側と復号側とで同一の値を用いる。IVの値は、第三者に知られてもよいので、IVは送信者と受信者との間で秘密に送る必要がない。IVの値を変えると、同じメッセージから異なった暗号文が生成される。

【0191】

図51は、CBCモードにおける暗号化の概要を示した概念図である。

図52は、CBCモードにおける復号化の概要を示した概念図である。

【0192】

図51、図52を参照して、ScRAMに一度に入力可能な平文長はレジスタREG1のサイズである4kビットである。したがって、4kビットよりも長い平文を処理する場合には、直前の暗号文ブロック C_i が初期値になるように制御レジスタに対して設定を行なう。

【0193】

本明細書の実施の形態では、SDRAMに本発明を適用した場合を例として示

したが、SDRAMに制限されるものではなく、非同期型のDRAM、たとえばEDO (Extended Data Out) DRAM等にも本発明を適用することも可能である。また、同期型の他のDRAM、たとえばDDR (Double Data Rate) 型のインタフェースを有するDRAM等であっても本発明を適用することが可能である。

【0194】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0195】

【発明の効果】

請求項1～3に記載の半導体記憶装置は、汎用的なメモリに対してデータ、アドレスおよび制御信号を与えるのと同様なシーケンスで信号を与えることで内蔵するロジック回路を制御することができ、既存のシステムに大きな変更を加える必要がなく、容易に制御することができる。

【0196】

請求項4に記載の半導体記憶装置は、請求項3に記載の半導体記憶装置の奏する効果に加えて、通常のメモリに対する読出を所定アドレスを指定して行なうことで、内蔵するロジック回路の動作状態を確認することができる。

【0197】

請求項5に記載の半導体記憶装置は、請求項3に記載の半導体記憶装置の奏する効果に加えて、内蔵するロジック回路が暗号処理を行なう場合に容易に制御を行なうことができる。

【0198】

請求項6に記載の半導体記憶装置は、請求項2に記載の半導体記憶装置の奏する効果に加えて、短時間で複数のモード設定を行なうことができる。

【0199】

請求項7に記載の半導体記憶装置は、請求項2に記載の半導体記憶装置の奏す

る効果に加えて、予約領域が様々なマイコンシステムに対応できる。

【0200】

請求項8に記載の半導体記憶装置は、請求項1に記載の半導体記憶装置の奏する効果に加えて、既存のメモリと置き換えて使用することが可能である。

【0201】

請求項9に記載の半導体記憶装置は、請求項1に記載の半導体記憶装置の奏する効果に加えて、内蔵メモリを有効に活用することができる。

【0202】

請求項10に記載の半導体記憶装置は、請求項9に記載の半導体記憶装置の奏する効果に加えて、特別な制御端子や命令がなくても内蔵メモリの保持データを内蔵ロジック回路に処理させることができる。

【0203】

請求項11～13に記載の半導体記憶装置の制御方法は、マイコンシステムにおいて、ロジック内蔵の半導体記憶装置を容易に制御することができる。

【0204】

請求項14～16に記載の半導体記憶装置は、最小限の制御端子の追加で、内蔵メモリにアドレスやデータを与える経路を有効に使用して、内蔵するロジック回路の制御を行なうことができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態1の半導体記憶装置1の構成を示したブロック図である。

【図2】 実施の形態1のロジック内蔵半導体記憶装置のメモリマップの例を示した図である。

【図3】 外部から入力される信号がロジック回路へ伝達される様子を説明するための図である。

【図4】 実施の形態1の半導体記憶装置の標準的なタイミングを説明するための波形図である。

【図5】 実施の形態1の変形例であるロジック内蔵DRAM10の構成を示すブロック図である。

【図 6】 図 5 に示したロジック内蔵 D R A M 1 0 のメモリマップを示した図である。

【図 7】 実施の形態 2 のロジック内蔵 D R A M 3 0 の構成を示すブロック図である。

【図 8】 実施の形態 2 のロジック内蔵 D R A M に適用されるシステムのメモリマップを示した図である。

【図 9】 図 7 の暗号演算ロジック 7 4 がサポートする暗号方式を示した図である。

【図 1 0】 レジスタに割当てられるデータ例を示した第 1 の図である。

【図 1 1】 レジスタに割当てられるデータ例を示した第 2 の図である。

【図 1 2】 レジスタに割当てられるデータ例を示した第 3 の図である。

【図 1 3】 レジスタに割当てられるデータ例を示した第 4 の図である。

【図 1 4】 レジスタに割当てられるデータ例を示した第 5 の図である。

【図 1 5】 レジスタに割当てられるデータ例を示した第 6 の図である。

【図 1 6】 レジスタに割当てられるデータ例を示した第 7 の図である。

【図 1 7】 レジスタに割当てられるデータ例を示した第 8 の図である。

【図 1 8】 レジスタに割当てられるデータ例を示した第 9 の図である。

【図 1 9】 本発明のロジック内蔵 D R A M 9 2 とマイクロコンピュータ 9 0 とが接続される様子を示した図である。

【図 2 0】 ロジック内蔵 D R A M の制御を説明するためのフローチャートである。

【図 2 1】 実施の形態 4 において割当てたメモリマップを示した図である。

【図 2 2】 実施の形態 5 のロジック内蔵 D R A M 1 1 1 の構成を示した図である。

【図 2 3】 実施の形態 5 におけるマイクロコンピュータシステムのメモリマップを示した図である。

【図 2 4】 実施の形態 5 のロジック内蔵 D R A M の制御を説明するための動作波形図である。

- 【図 2 5】 実施の形態 5 の変形例を説明するための図である。
- 【図 2 6】 実施の形態 5 の変形例の動作を説明するための動作波形図である。
- 【図 2 7】 S c R A M 2 0 0 の構成を示したブロック図である。
- 【図 2 8】 制御レジスタの設定に応じたメモリマップの状態変化を説明するための図である。
- 【図 2 9】 図 2 7 に示したモードレジスタ 2 0 8 を説明するための第 1 図である。
- 【図 3 0】 図 2 7 に示したモードレジスタ 2 0 8 を説明するための第 2 図である。
- 【図 3 1】 図 2 7 に示したモードレジスタ 2 0 8 を説明するための第 3 図である。
- 【図 3 2】 S c R A M の暗号制御エントリ・エグジットに関連する状態遷移図である。
- 【図 3 3】 制御レジスタアクセスの一例を示した動作波形図である。
- 【図 3 4】 制御レジスタのアドレスマップを示した第 1 図である。
- 【図 3 5】 制御レジスタのアドレスマップを示した第 2 図である。
- 【図 3 6】 制御レジスタのアドレスマップを示した第 3 図である。
- 【図 3 7】 制御レジスタのアドレスマップを示した第 4 図である。
- 【図 3 8】 信号 C R Y P を与える端子を制御可能なシステムを説明するための図である。
- 【図 3 9】 C R Y P 端子を制御不可能なシステムについて説明するための第 1 の図である。
- 【図 4 0】 C R Y P 端子を制御不可能なシステムについて説明するための第 2 の図である。
- 【図 4 1】 制御レジスタへの設定の説明をするための動作波形図である。
- 【図 4 2】 暗号化処理の基本単位について示した第 1 の概略図である。
- 【図 4 3】 暗号化処理の基本単位について示した第 2 の概略図である。
- 【図 4 4】 暗号化処理の基本単位について示した第 3 の概略図である。

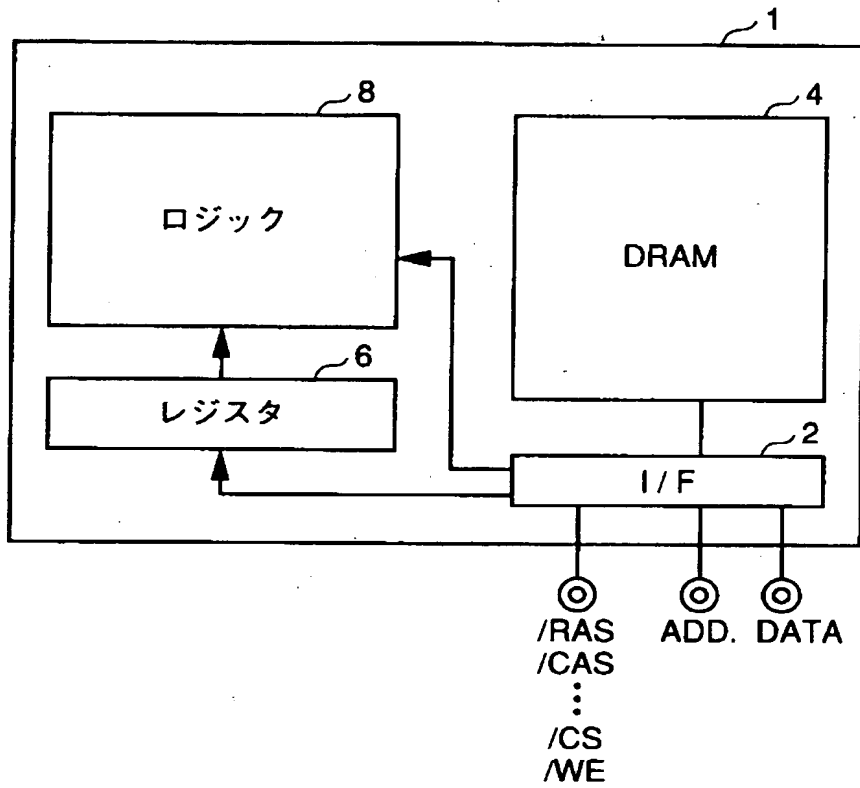
- 【図 4 5】 復号化処理の単位について示した第 1 の概略図である。
- 【図 4 6】 復号化処理の単位について示した第 2 の概略図である。
- 【図 4 7】 復号化処理の単位について示した第 3 の概略図である。
- 【図 4 8】 ECBモードについて説明するための第 1 図である。
- 【図 4 9】 ECBモードについて説明するための第 2 図である。
- 【図 5 0】 CBCモードの演算を説明するための図である。
- 【図 5 1】 CBCモードにおける暗号化の概要を示した概念図である。
- 【図 5 2】 CBCモードにおける復号化の概要を示した概念図である。
- 【図 5 3】 従来の、シンクロナスダイナミックランダムアクセスメモリ (SDRAM) のピン配置を示した図である。
- 【図 5 4】 SDRAMの端子名と機能とを示した図である。
- 【図 5 5】 従来のロジック内蔵DRAMの構成を示す図である。

【符号の説明】

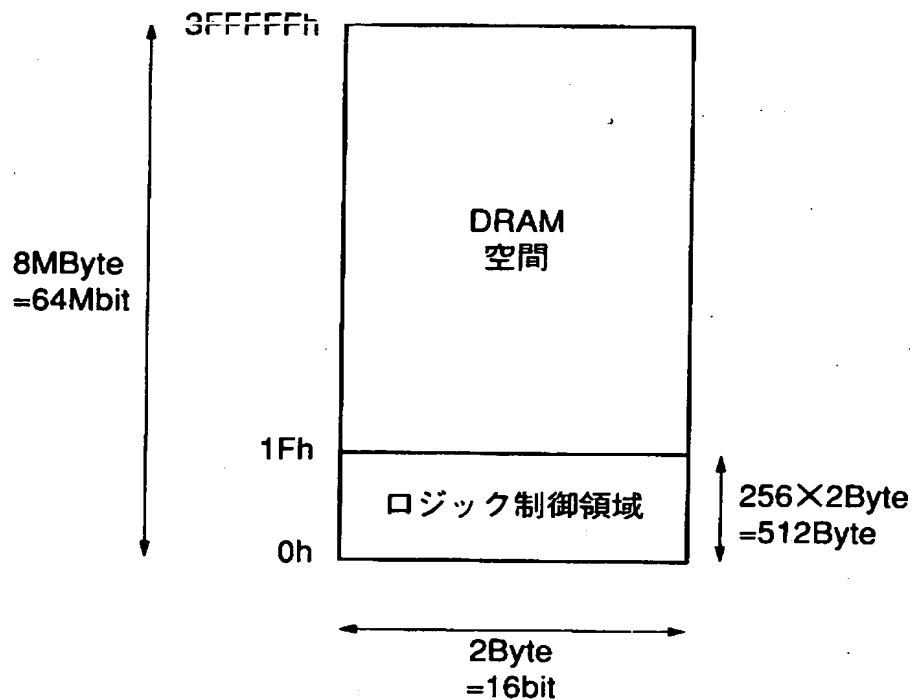
1 半導体記憶装置、2 インターフェイス部、3 バッファ、5 デコード回路、6, 14, 16, 116, 126 レジスタ、8, 118 ロジック回路、10, 30, 92, 111, 121 ロジック内蔵DRAM、12 インターフェイス部、18, 20 ロジック回路、32 SDRAM部、34 ロジック部、36 インターフェイス部、38 DRAMコア、40 制御信号入力回路、42 制御回路、44 クロックバッファ、46 アドレスバッファ、48 マルチプレクサ、50 モードレジスタ、52 入出力回路、54 メモリセルアレイ、56 ロウデコーダ、60 ライトドライバ、72 レジスタ部、74 暗号演算ロジック、76 セレクタ、78 制御レジスタ、80 モードレジスタ、82 ステータスレジスタ、84, 86 データレジスタ、90, 132 マイクロコンピュータ、94, 134 CPUコア、96 キャッシュメモリ、98, 136 メモリコントローラ、100, 142 外部バスインターフェイス回路、102 内部バス、121 半導体記憶装置、130 ATD回路、140 マルチプレクス回路。

【書類名】 図面

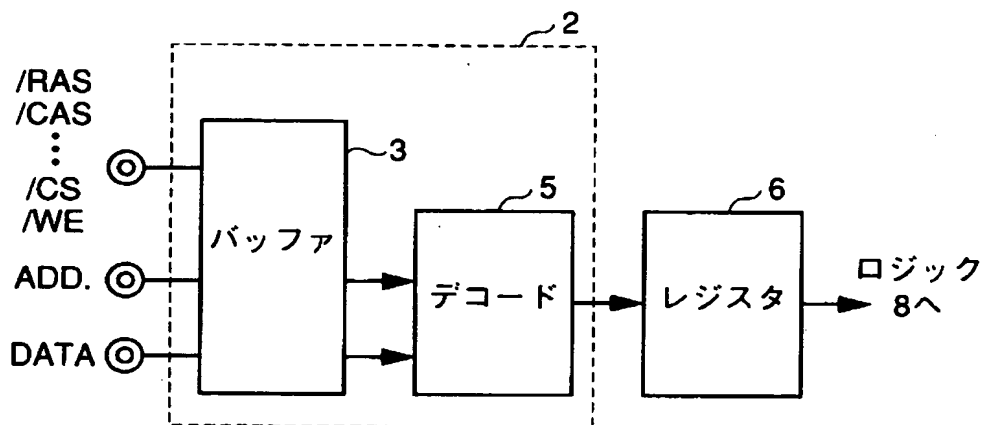
【図 1】



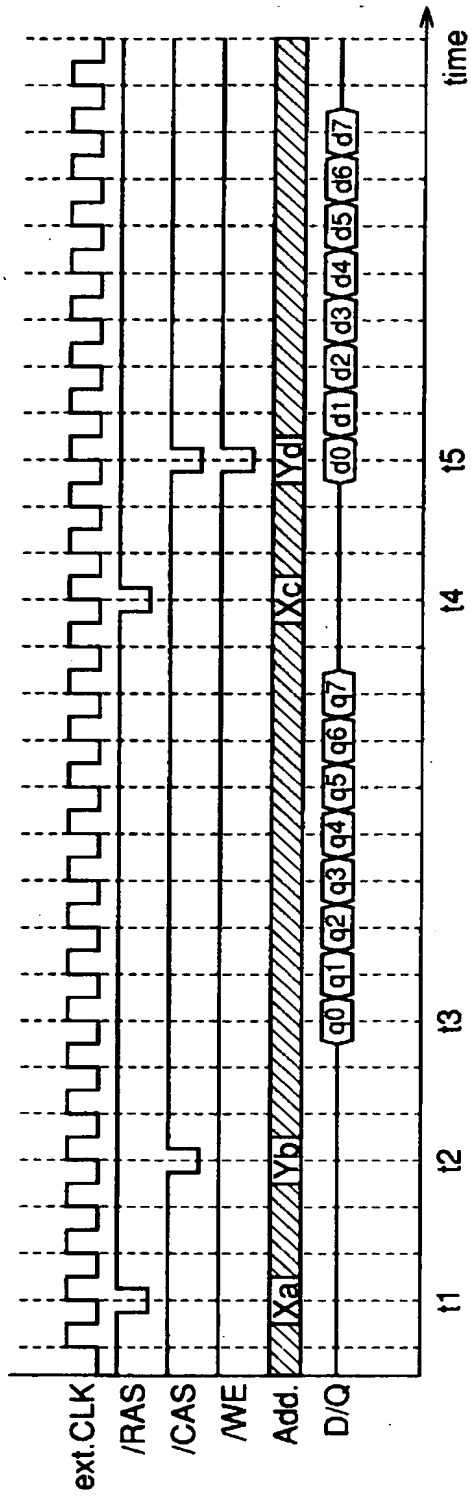
【図 2】



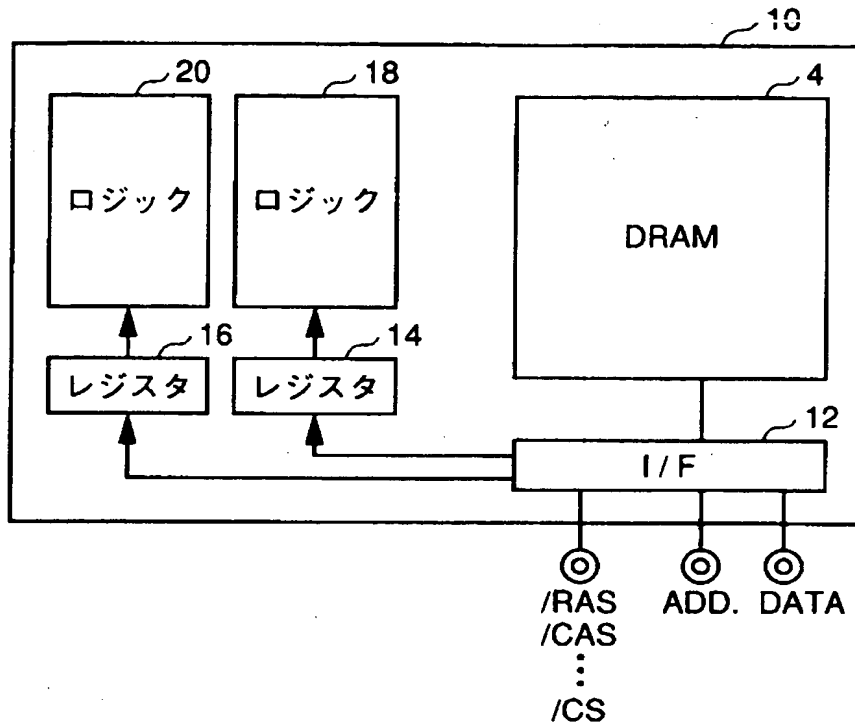
【図 3】



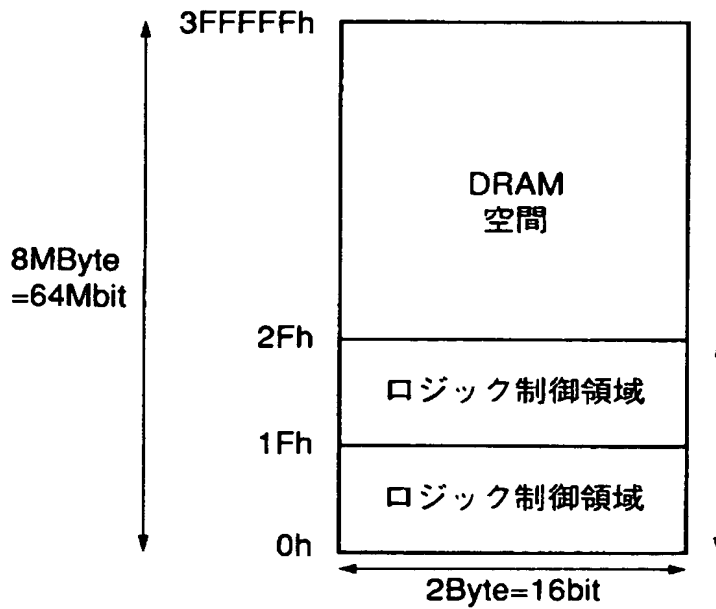
【図 4】



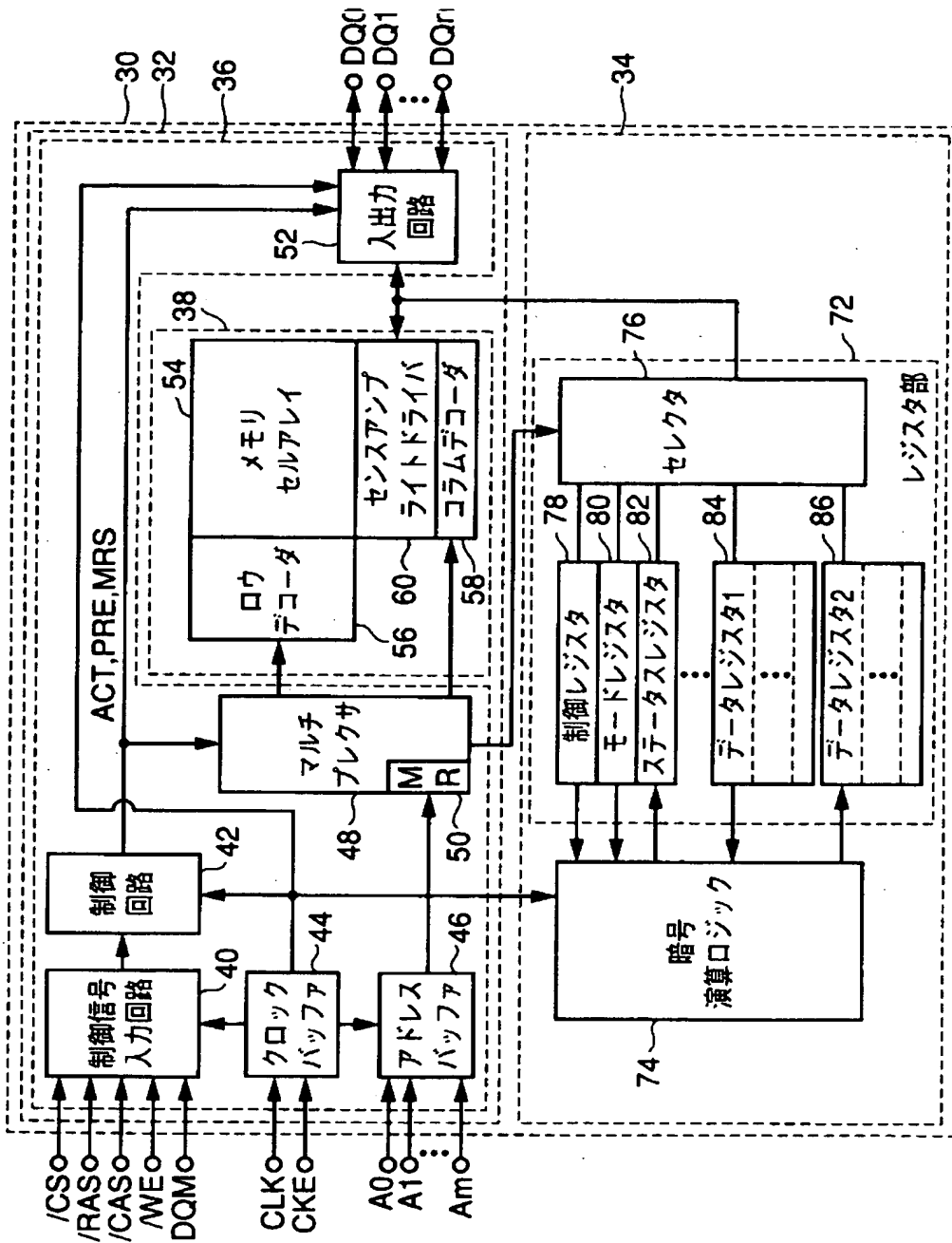
【図 5】



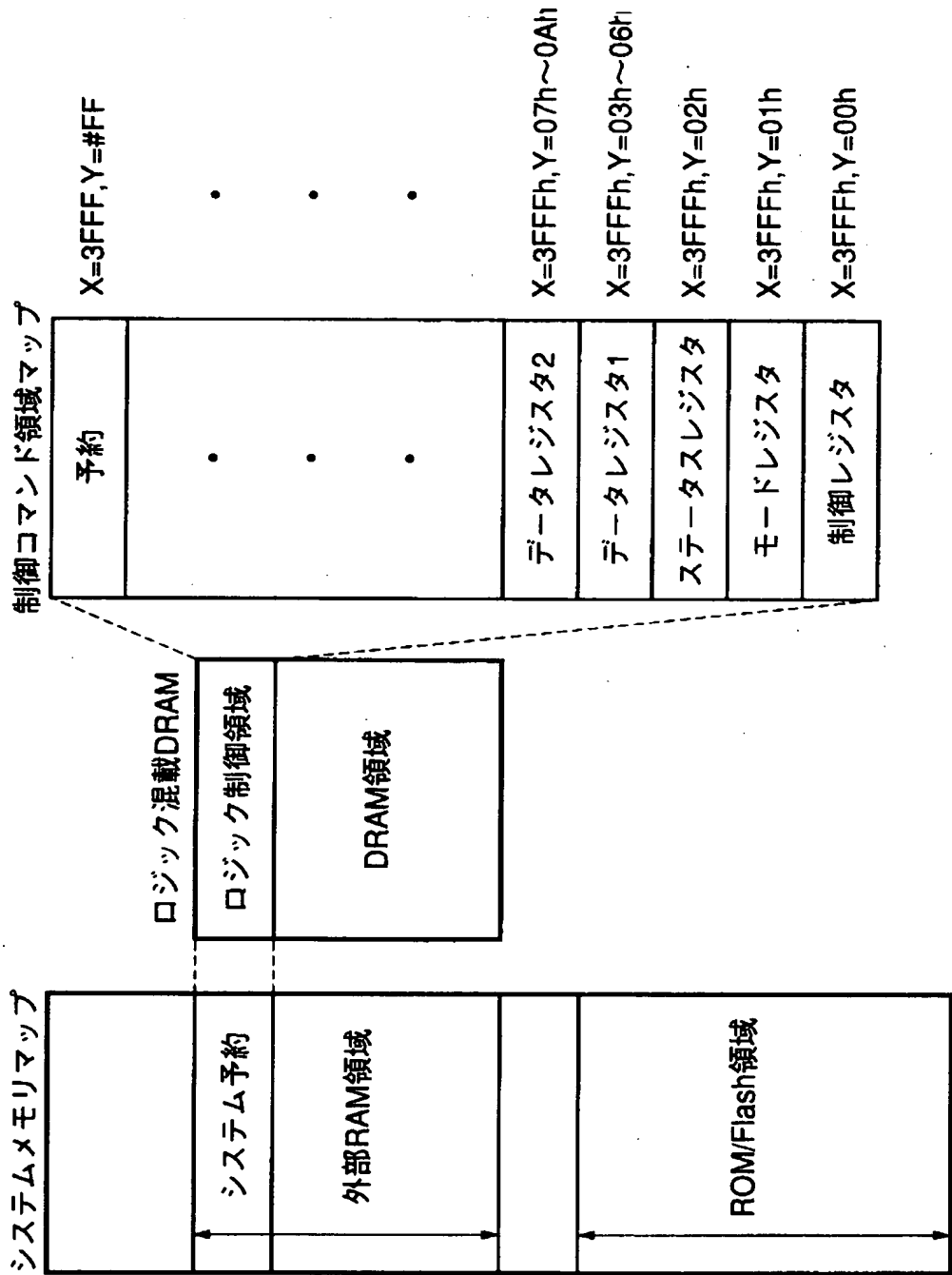
【図 6】



【図7】



【図 8】



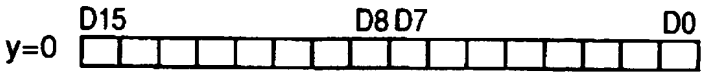
【図 9】

公開鍵暗号方式	秘密鍵暗号方式	
	DES Triple DES	ブロック暗号化モード ECB:Electric Code Book CBC:Cipher Block Chaining OFB:Output Feed Back CFB:Cipher Feed Back
RSA		

サポートする暗号方式

【図 1 0】

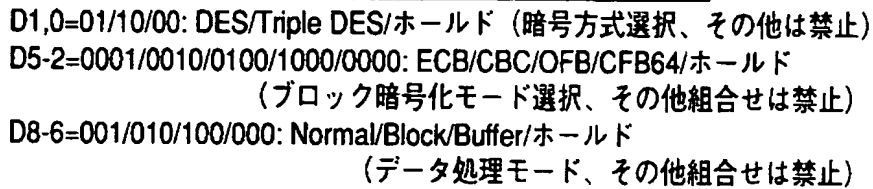
・公開鍵と秘密鍵方式共通



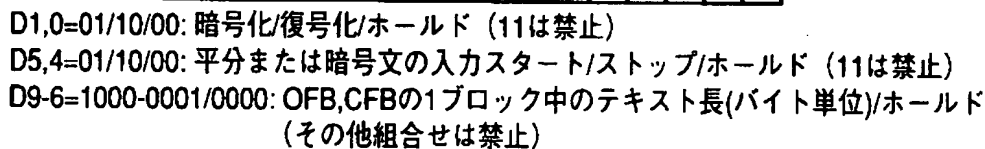
D0 =1: 暗号機能リセット

D1 =1: 暗号処理中を示すフラッグ (0を確認してからアクセスする)

・秘密鍵方式の制御



【図 12】



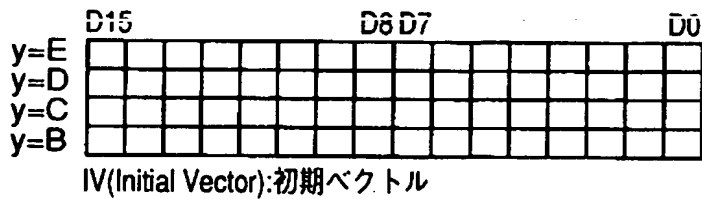
【図 13】



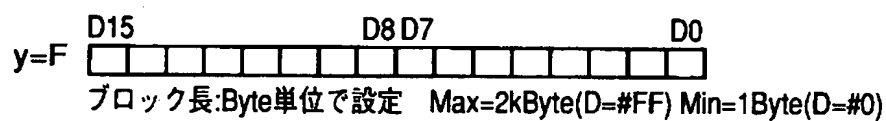
【図 14】



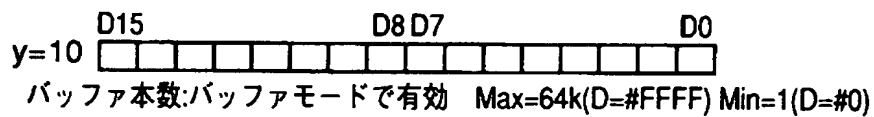
【図 1 5】



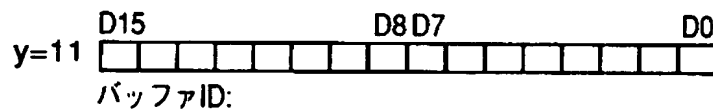
【図 1 6】



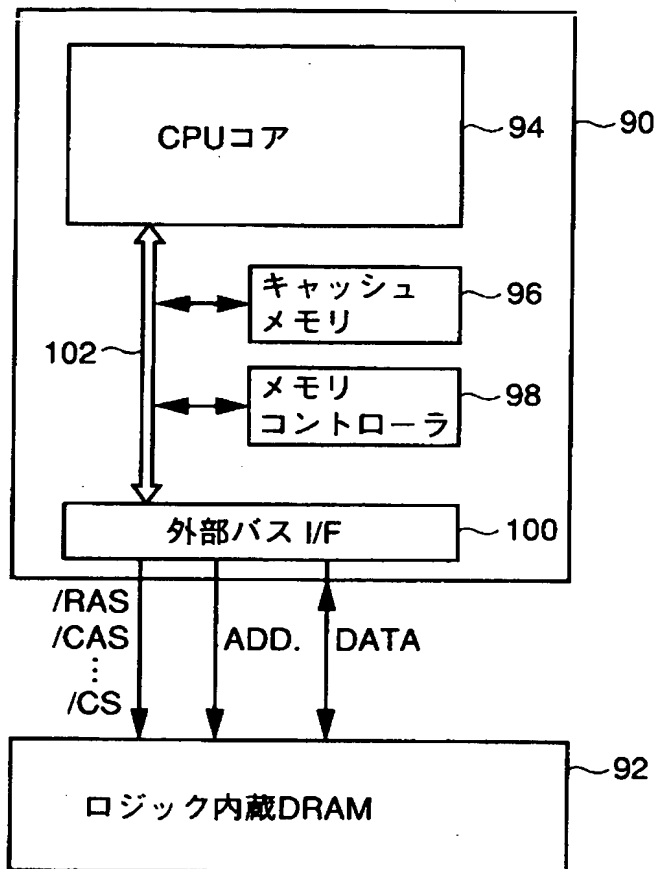
【図 1 7】



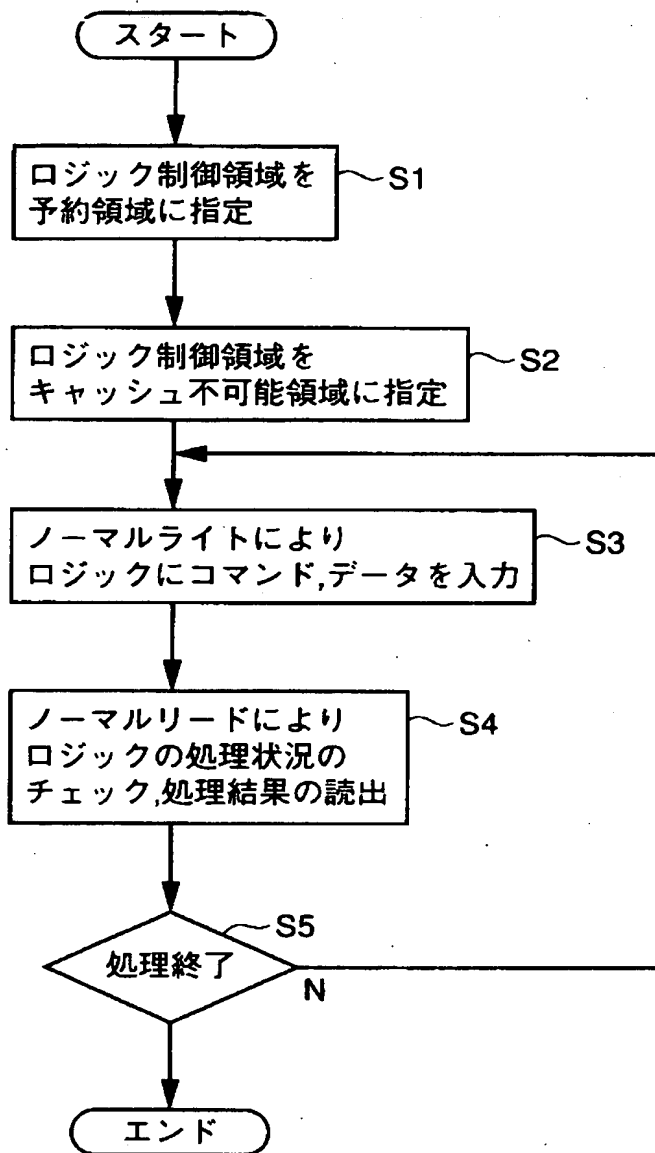
【図 1 8】



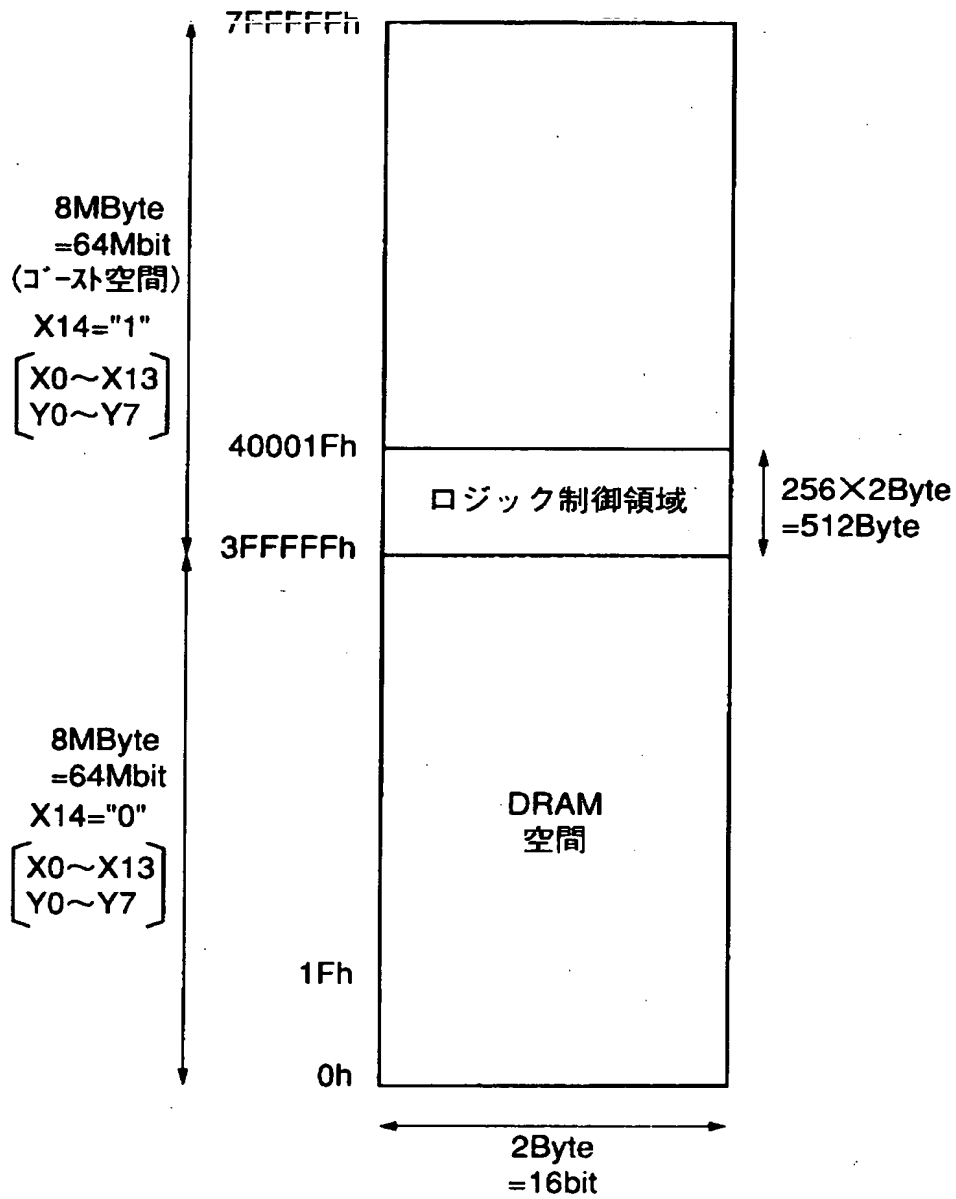
【図 1 9】



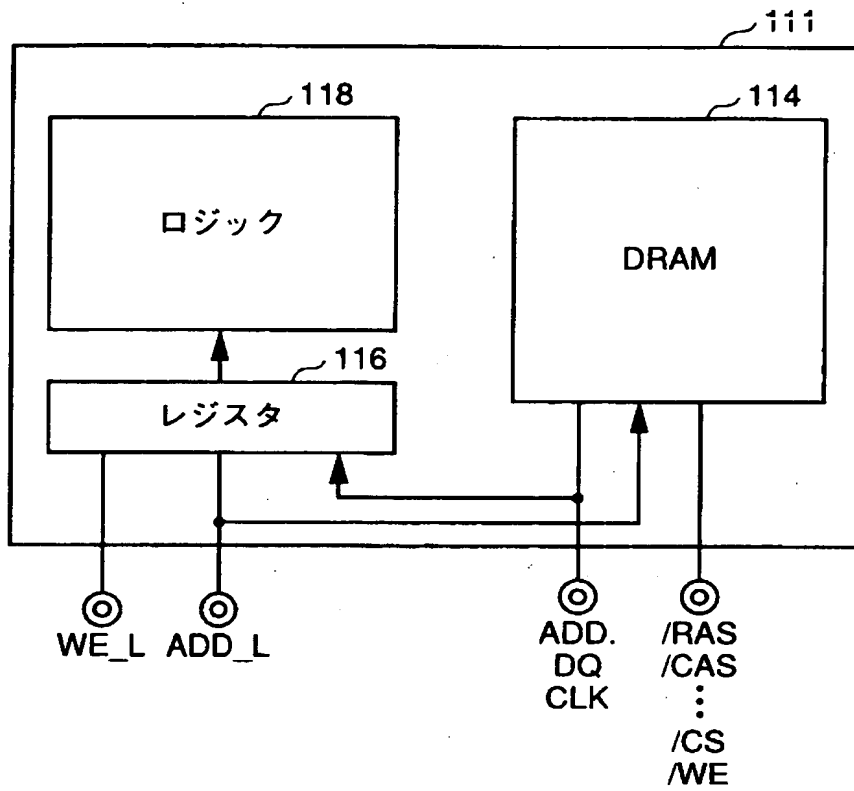
【図 20】



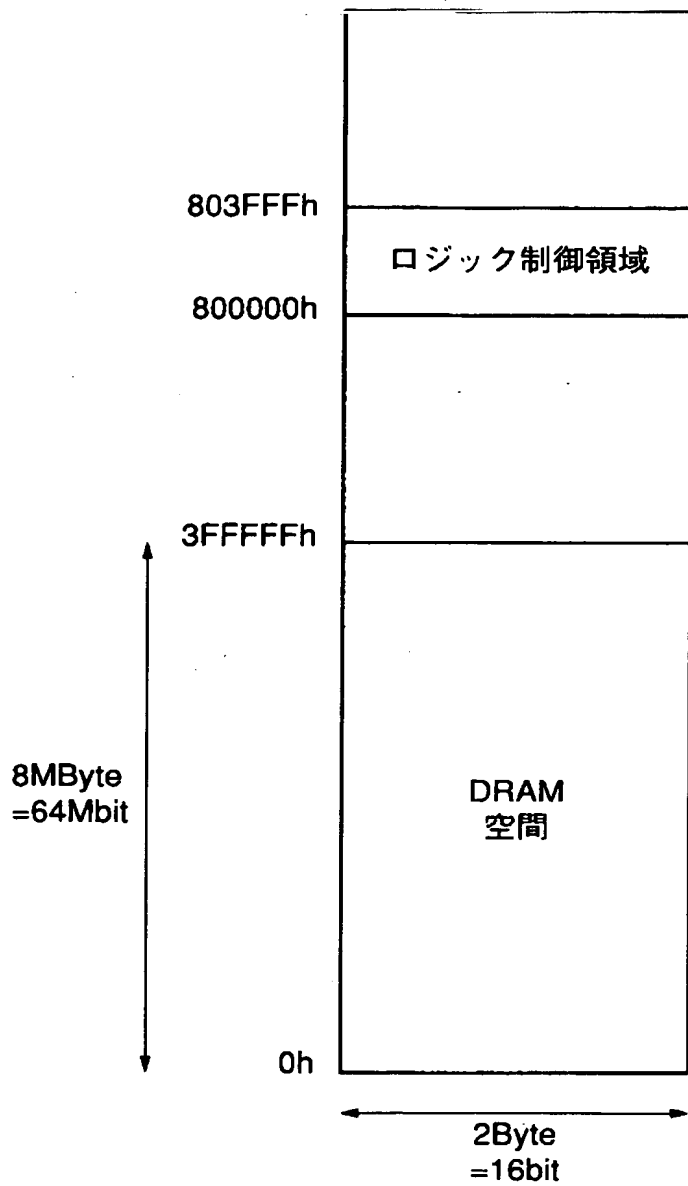
【図 2 1】



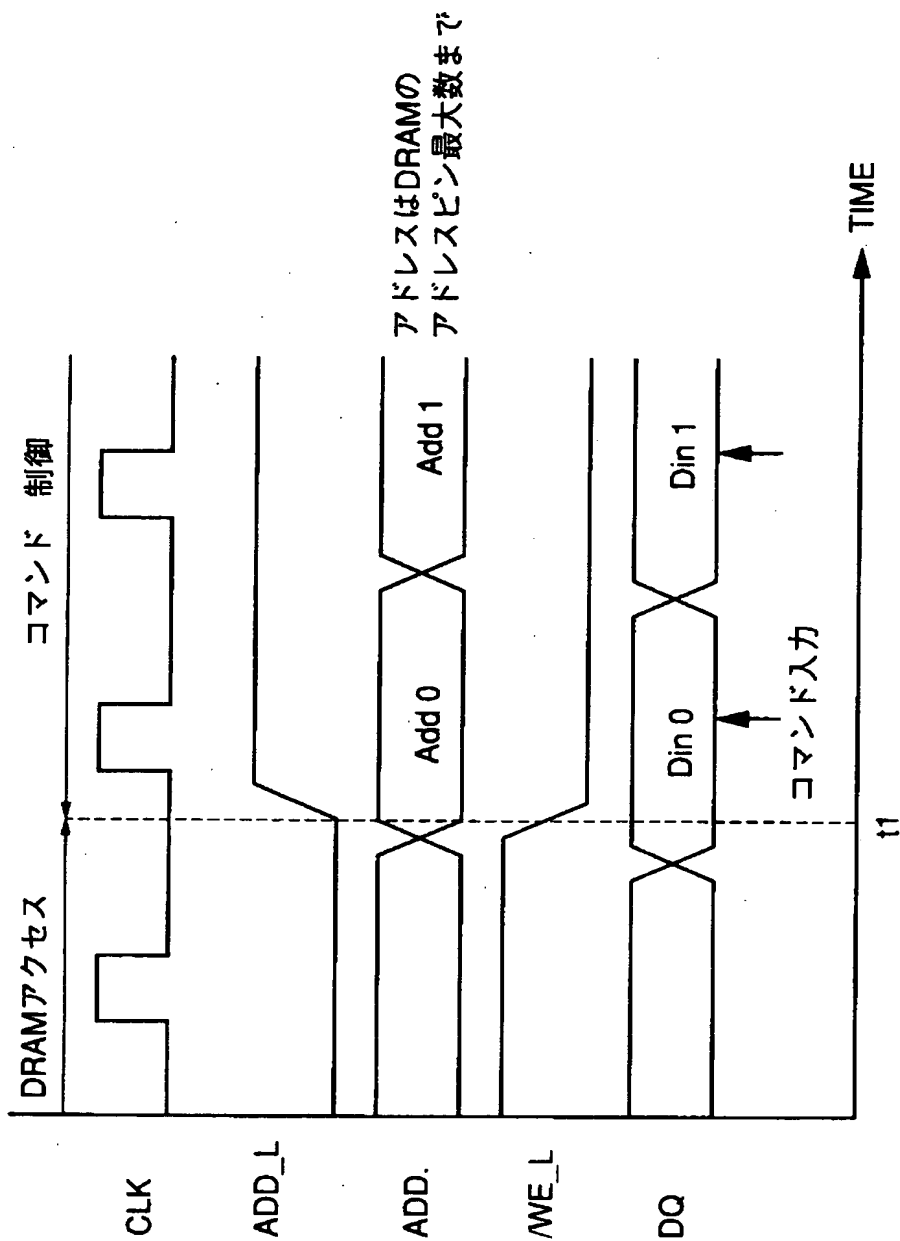
【図 2 2】



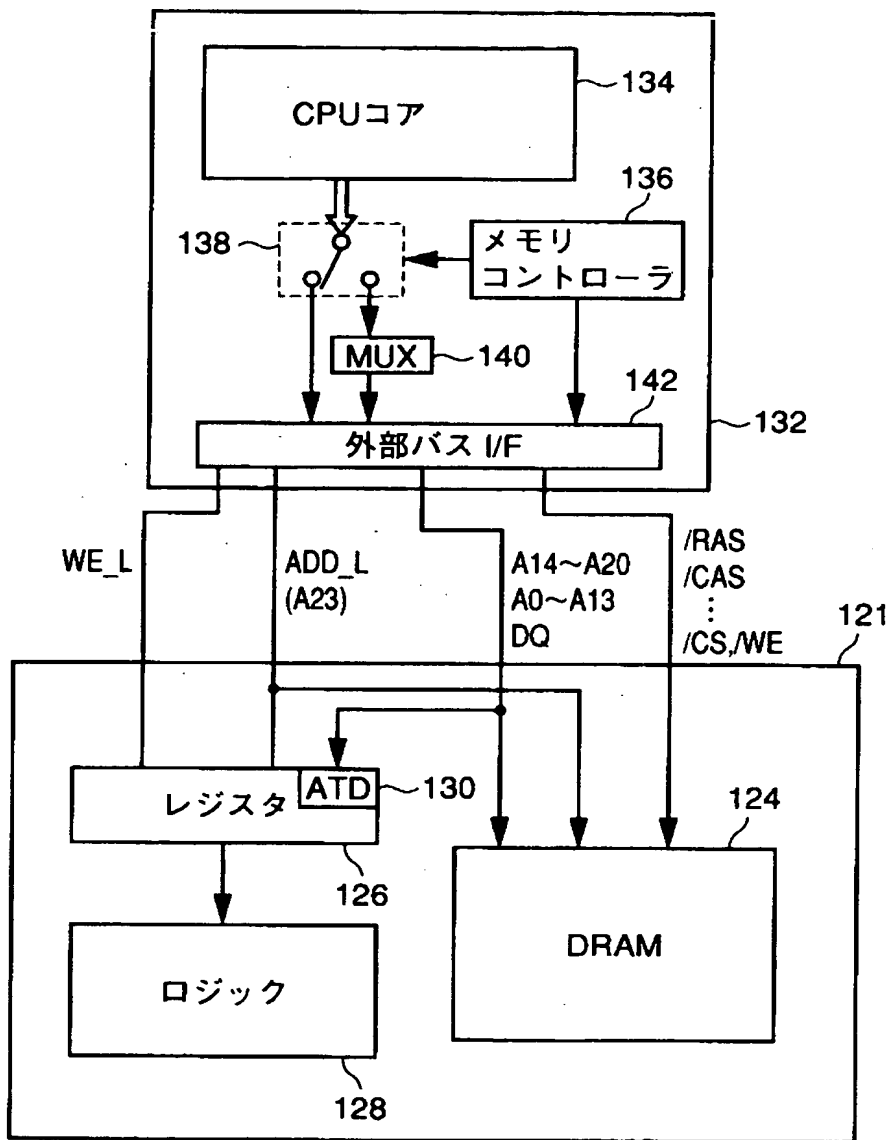
【図 2 3】



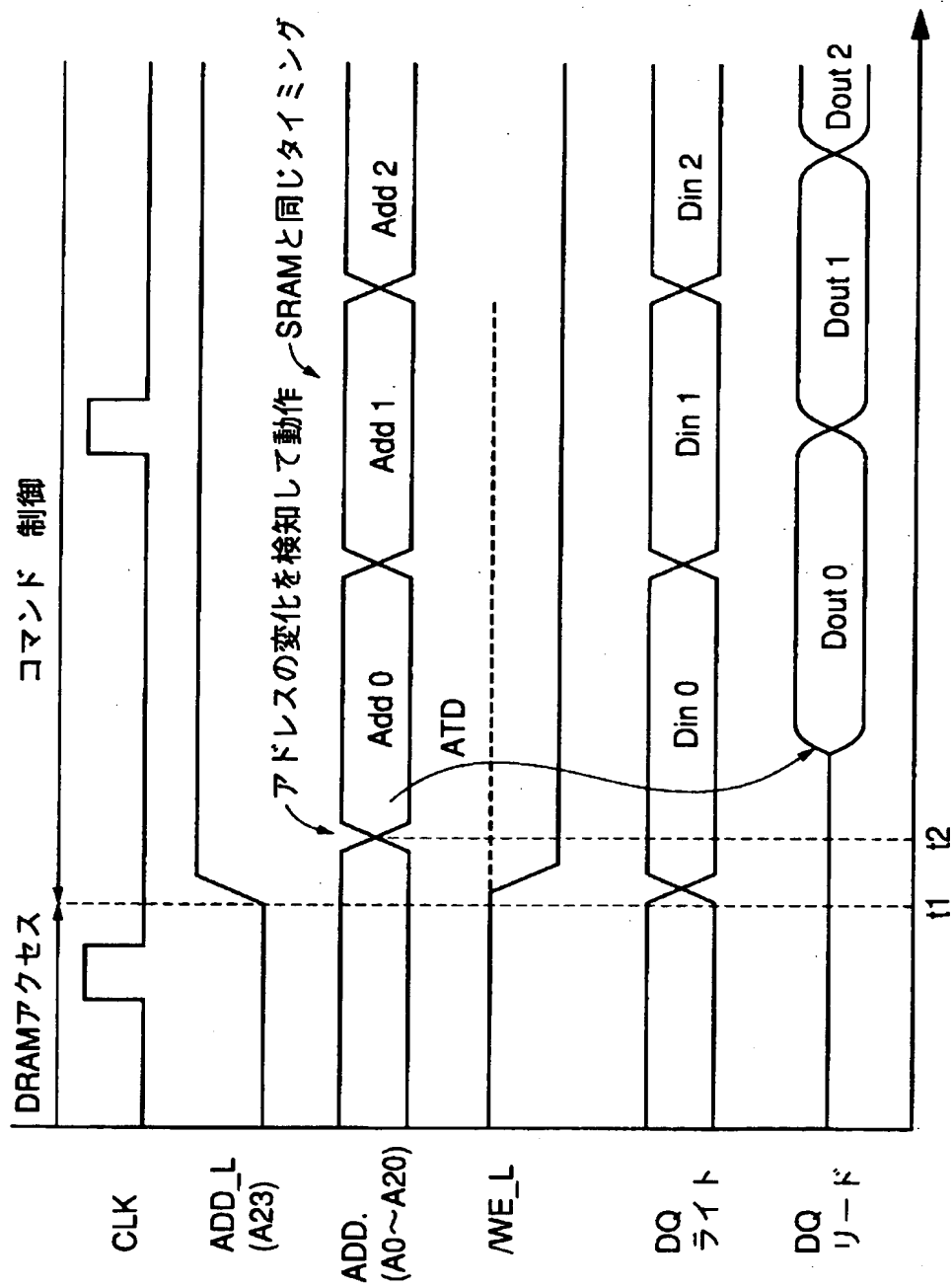
【図 24】



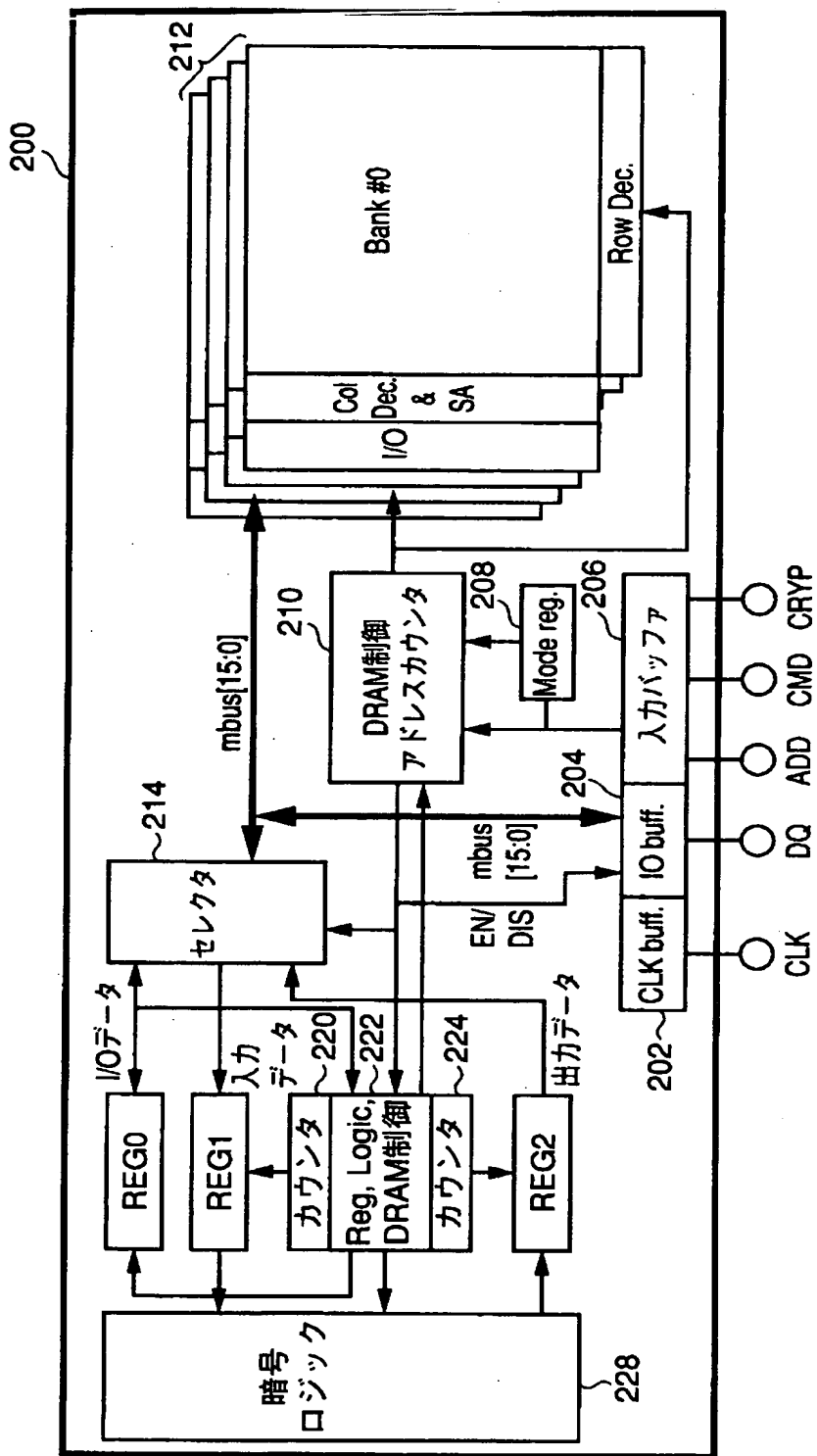
【図 25】



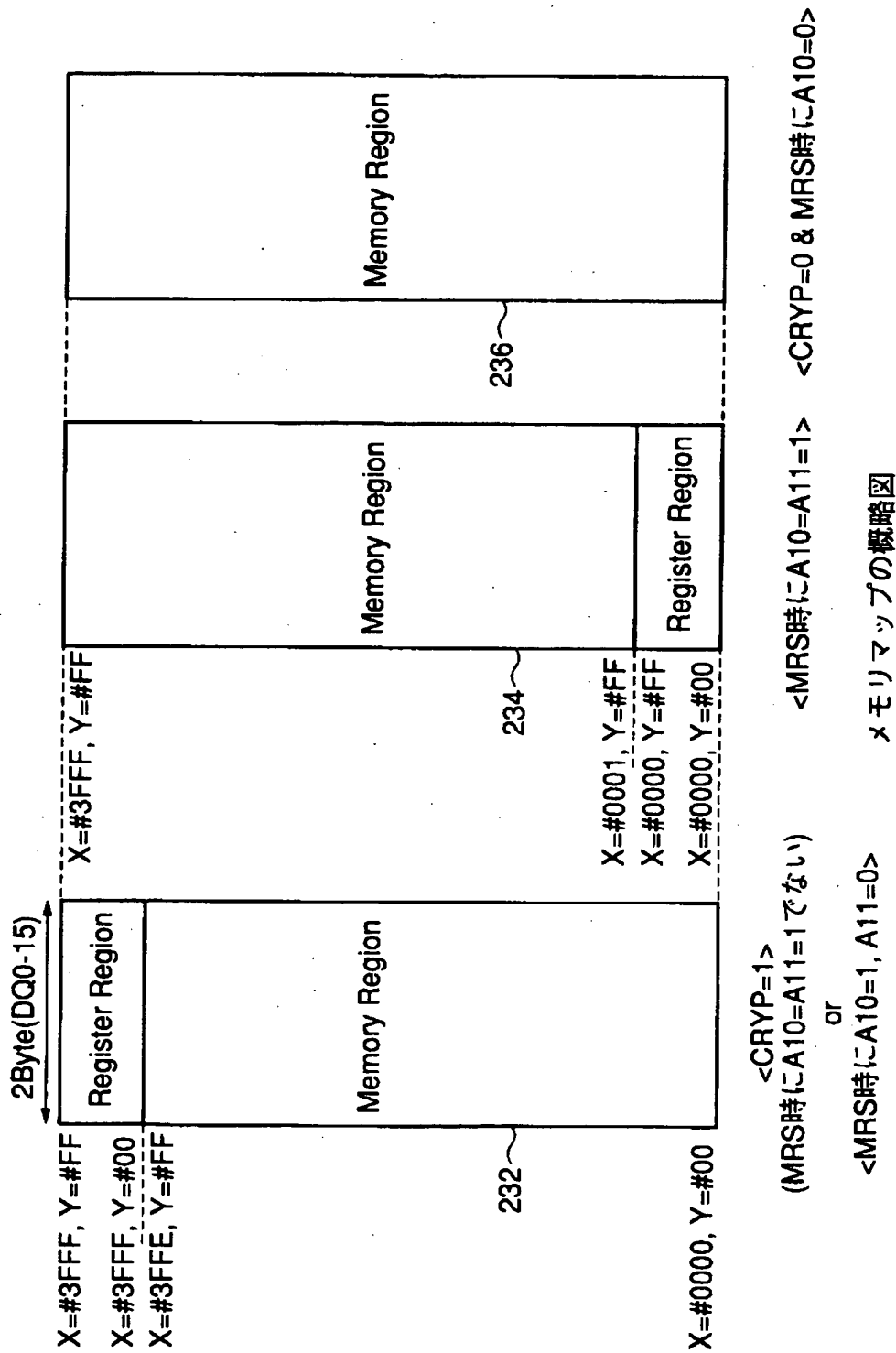
【図 26】



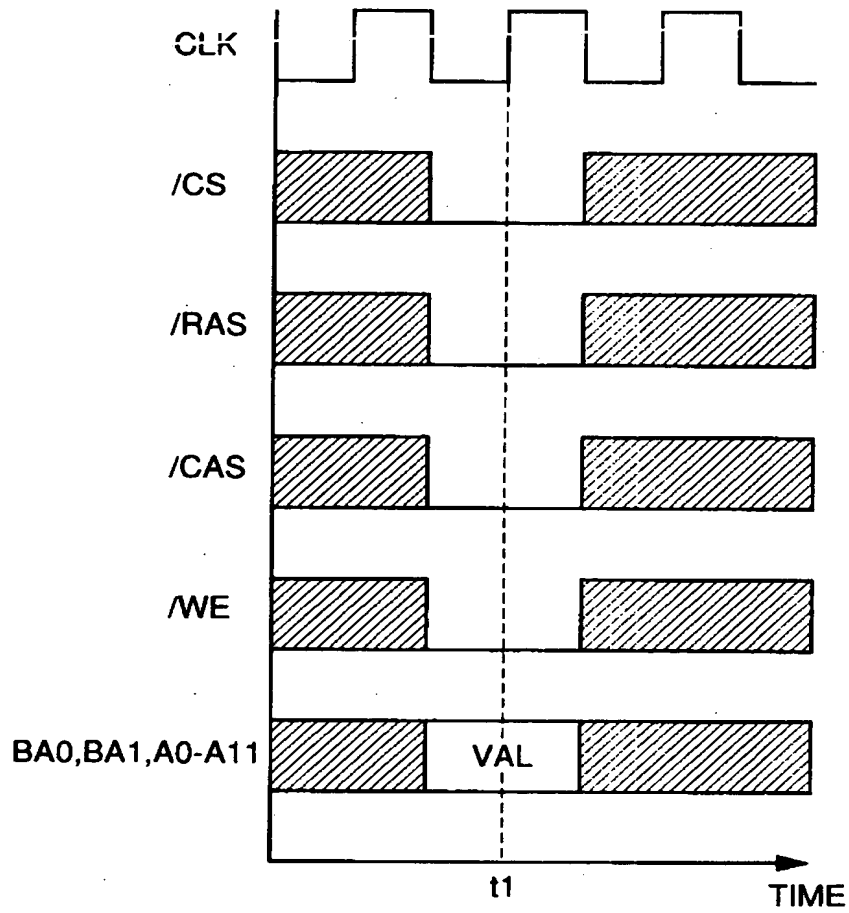
【図 27】



【図 2 8】



【図 2 9】



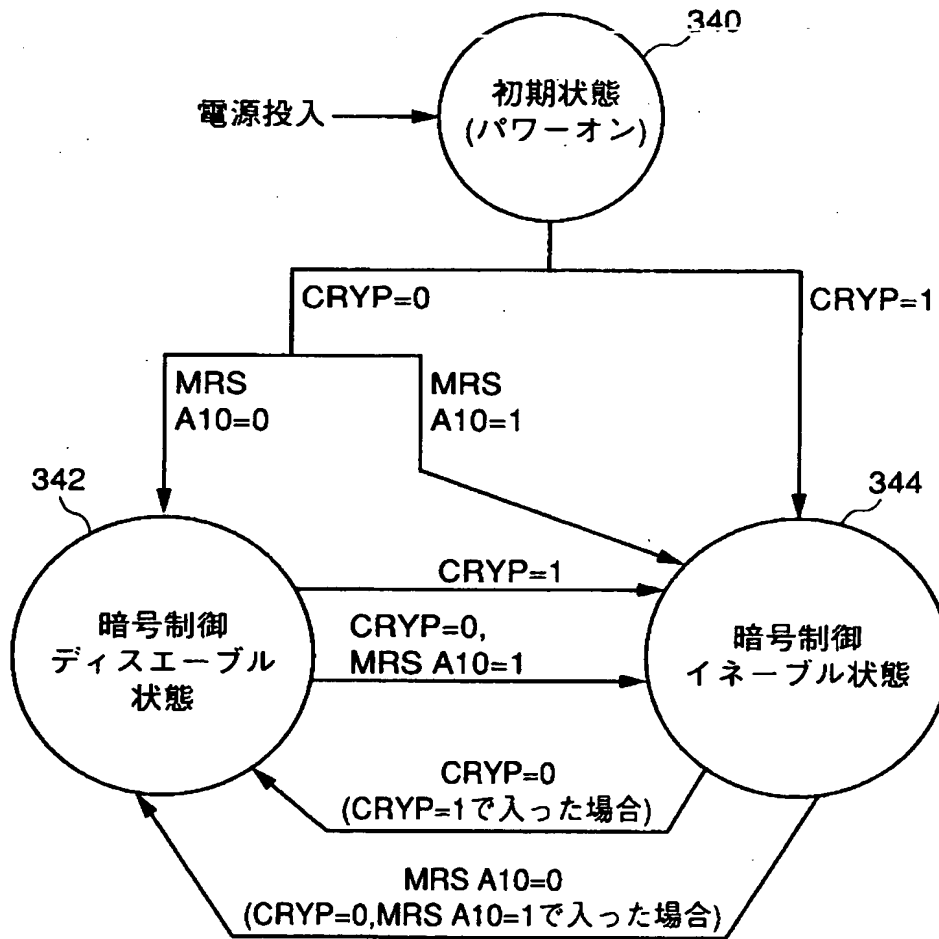
【図 3 0】

BA0	BA1	A11	A10	A9	A8	A7	A6	A5	A4	A3	A2	A1	A0
					0	0							

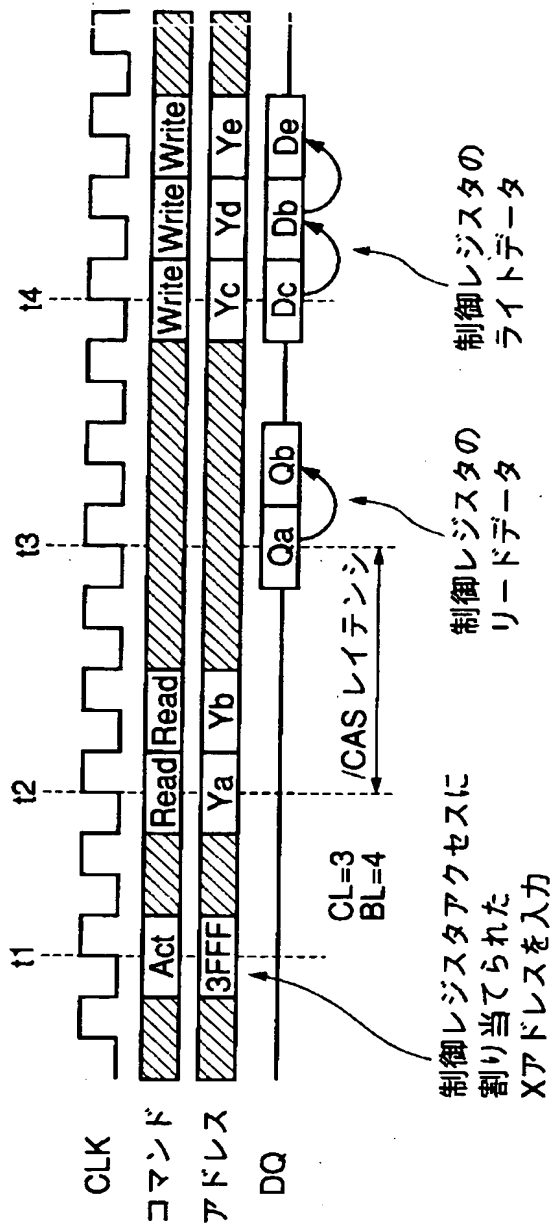
【図 3 1】

Bits	Name	Description	
A2..0	Burst Length	000	1
		001	2
		010	4
		011	8
		100	R
		101	R
		110	R
		111	Full Page
A3	Burst Type	0	Sequential
		1	Interleaved
A6..4	CAS Latency	000	R
		001	R
		010	2
		011	3
		1XX	R
A9	Write Mode	0	Burst
		1	Single Bit
A10	Control Reg. Access	0	Disable
		1	Enable
A11	Control Reg. Address	0	X=3FFF
		1	X=0
BA1	Low Power Mode	0	Disable
		1	Enable
BA0	Low Clock Frequency	0	Disable
		1	Enable

【図 3 2】



【図 33】



【図 3 4】

Col. Add.	Bits	Name		Description	Access
h00	D0	Software Reset	1	Reset	W
	D1	Flag	0	Done	R
			1	Processing	R
	D2	Change add for reg. cont.	1	X=h3FFF	W
h01	D3	Change add for reg. cont.	1	X=h0	W
	D4	EOF(End of File)	1		W
	D1	Partial Refresh	1/0	Bank0 Enable/Disable	W
	D2		1/0	Bank1 Enable/Disable	W
	D3		1/0	Bank2 Enable/Disable	W
	D4		1/0	Bank3 Enable/Disable	W
	D5	LP Mode	1/0	Enable/Disable	W
	D6	Low Clock Frequency	1/0	Enable/Disable	W

【図35】

Col. Add.	Bits	Name	Description	Access
h02	D1..0	Secret Cryp. Mode	00 Hold	W
			01 DES-56	W
			10 Triple DES-112	W
			11 Triple DES-168	W
	D5..2	Block Cryp. Mode	0000 Hold	W
			0001 ECB	W
			0010 CBC	W
			0100 OFB	W
	D9..6	Enabled bank set in Reg-DRAM transfer mode	1000 CFB-64	W
			0000 All Bank Disable	W
			1/0 Bank0 Enable/Disable	W
			1/0 Bank1 Enable/Disable	W
	D10	Simultaneous transfer	1/0 Bank2 Enable/Disable	W
			1/0 Bank3 Enable/Disable	W
			1/0 Enable/Disable	W

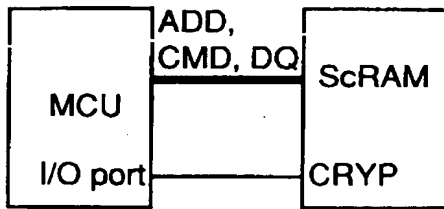
【図 3 6】

Col. Add.	Bits	Name	Description	Access
h03	D1..0	ENC/DEC	00 Hold	W
			01 Encryption	W
			10 Decryption	W
			11 RFU	W
	D2	Counter of reg1	Reset	W
	D3	Counter of reg2	Reset	W
	D4	IV Load	Previous output	W
	D8..5	Text length per block	1 IV Load	W
			0000 Hold	W
			Else (D8..5)x1Byte	W
h04	D15..0	Reg.1 Access	Write Data: D15..0	W
h05	D15..0	Reg.2 Access	Read Data: D15..0	R
h06	D0	Reg-DRAM transfer	Mode entry	W
	D1		Mode exit	W
	D2		Counter reset of reg1	W
	D3		Counter reset of reg1	W

【図 3 7】

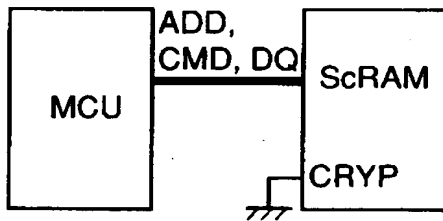
Col. Add.	Bits	Name	Description	Access
h13-h10	D15..0	Key1 for DES, Triple DES	LSB: h10[D0] USB: h13[D15] Key1 Input	W
h17-h14	D15..0	Key2 for Triple DES	LSB: h14[D0] USB: h17[D15] Key2 Input	W
h1B-h18	D15..0	Key3 for Triple DES-168	LSB: h18[D0] USB: h17B[D15] Key3 Input	W
h1F-h1C	D15..0	Initial Vector (IV)	LSB: h1C[D0] USB: h1F[D15] IV Input	W
hFF-h20	D15..0	Reserved		

【図 3 8】



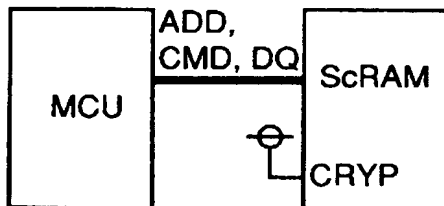
CRYP端子をI/O portで制御

【図 3 9】



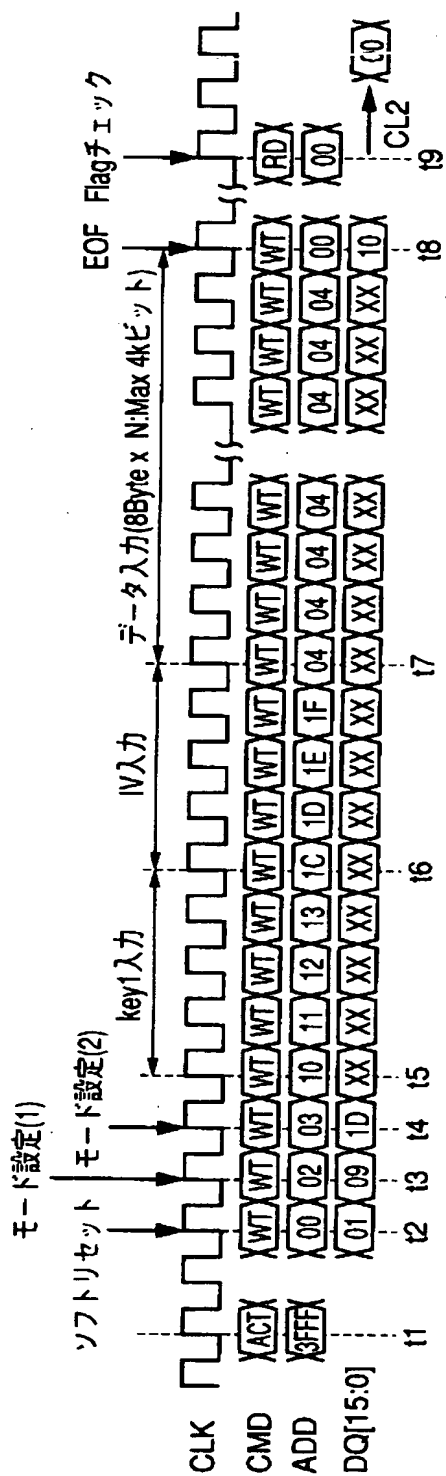
CRYP端子をL固定

【図 4 0】



CRYP端子をH固定

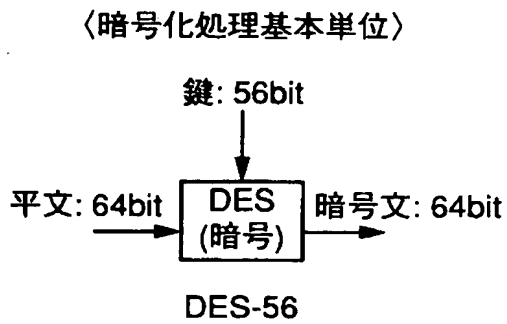
【図 4 1】



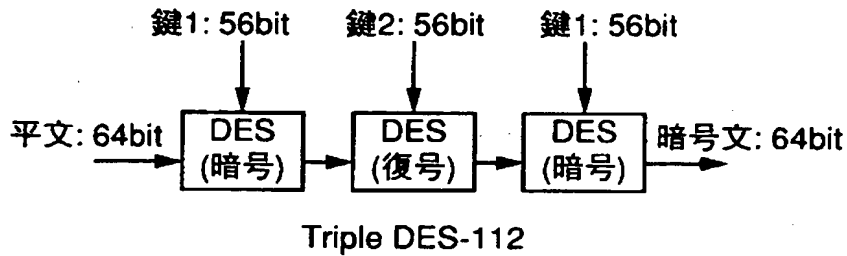
モード設定(1): DES-56,CBCモード

モード設定(2): 暗号化、Reg1,2のアドレスカウンタリセット、IVロード

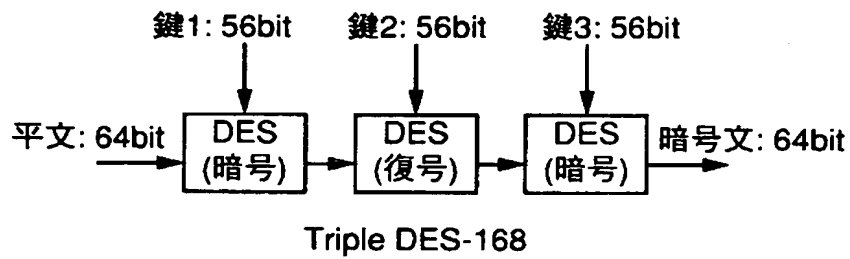
【図 4 2】



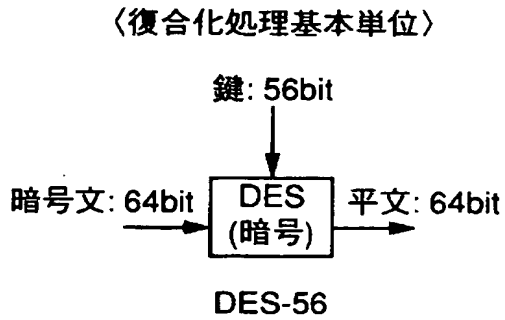
【図 4 3】



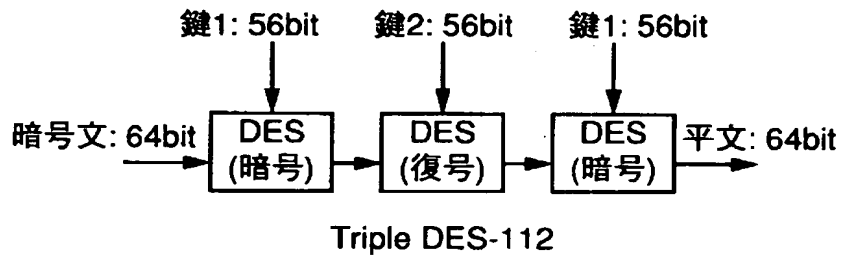
【図 4 4】



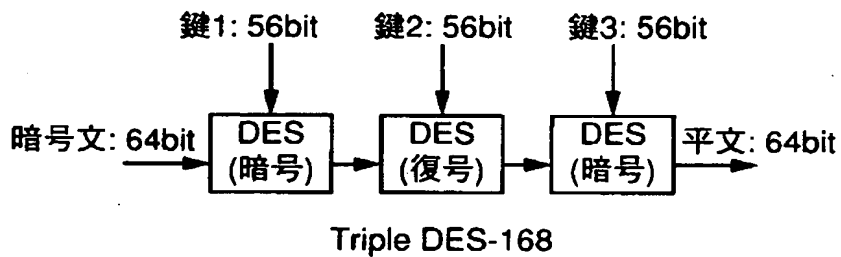
【図 4 5】



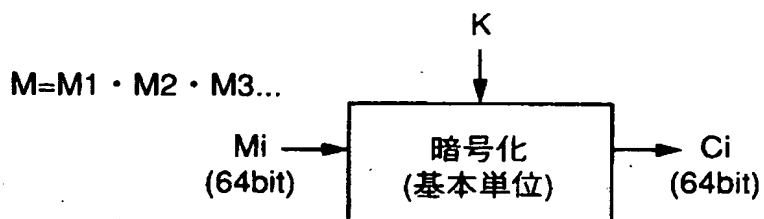
【図 4 6】



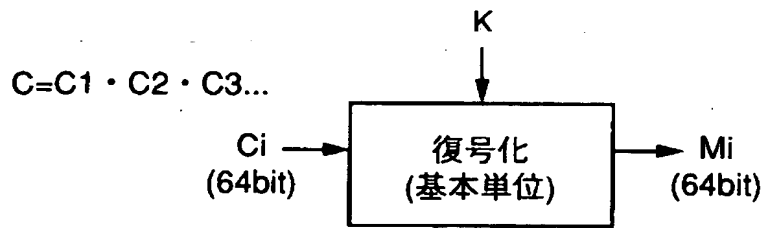
【図 4 7】



【図 4 8】



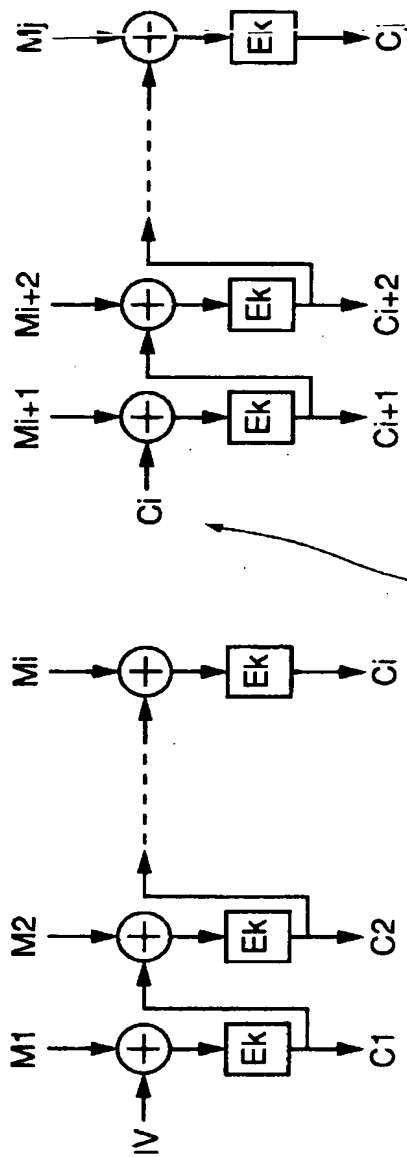
【図 4 9】



【図 5 0】

$$\begin{aligned}
 C_1 &= E_k (M_1 \oplus IV) \\
 C_i &= E_k (M_i \oplus C_{i-1}) \quad (i=2,3,\dots) \\
 M_1 &= D_k (C_1) \oplus M_1 \\
 M_i &= D_k (C_i) \oplus C_{i-1} \quad (i=2,3,\dots)
 \end{aligned}$$

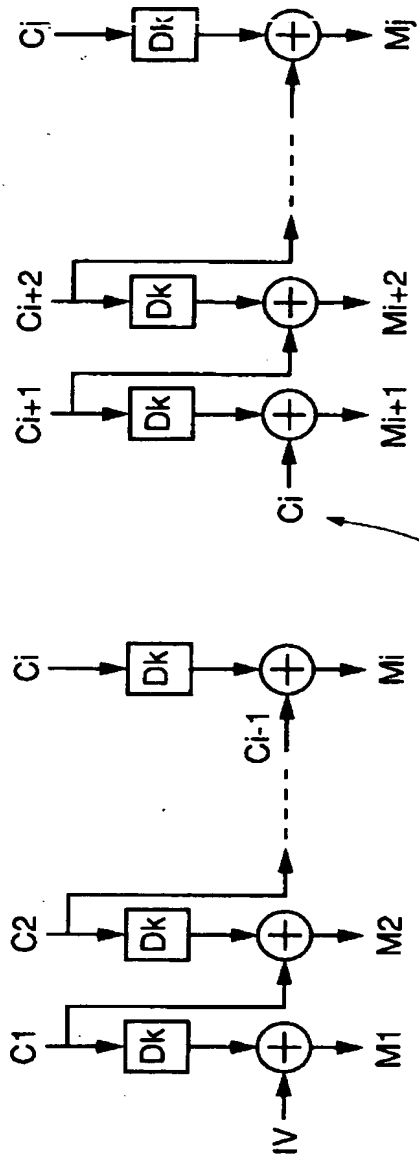
【図 5 1】



レジスタ1より平文Mが長い場合は、
初期値を直前の暗号文Ciにする。

〈CBCモードにおける暗号化の概要〉

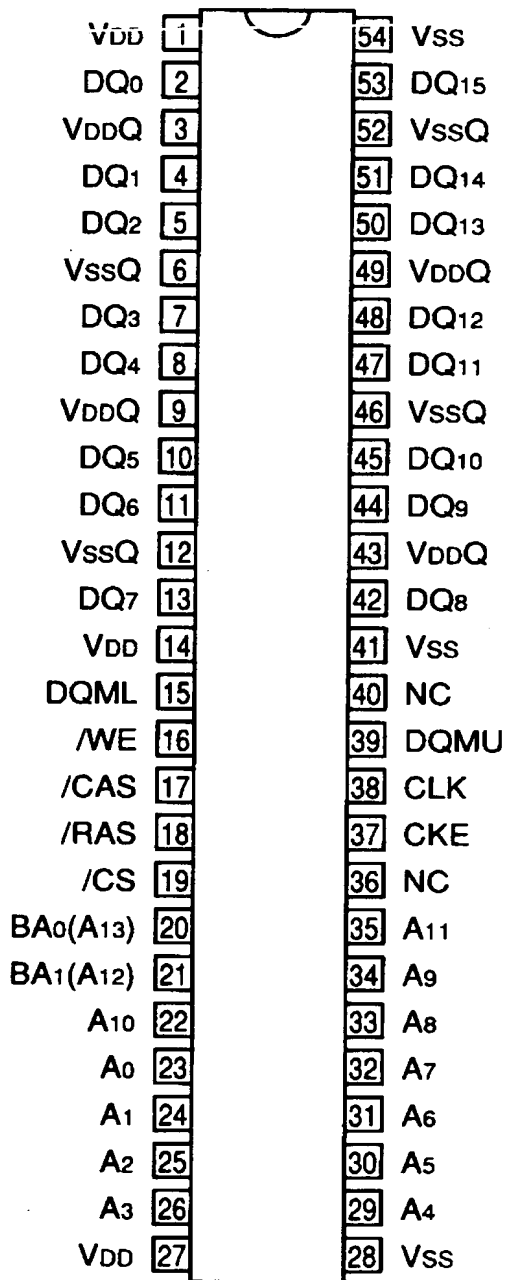
【図 5 2】



レジスタ1より平文Mが長い場合は、
初期値を直前の暗号文Cにする。

〈CBCモードにおける復号化の概要〉

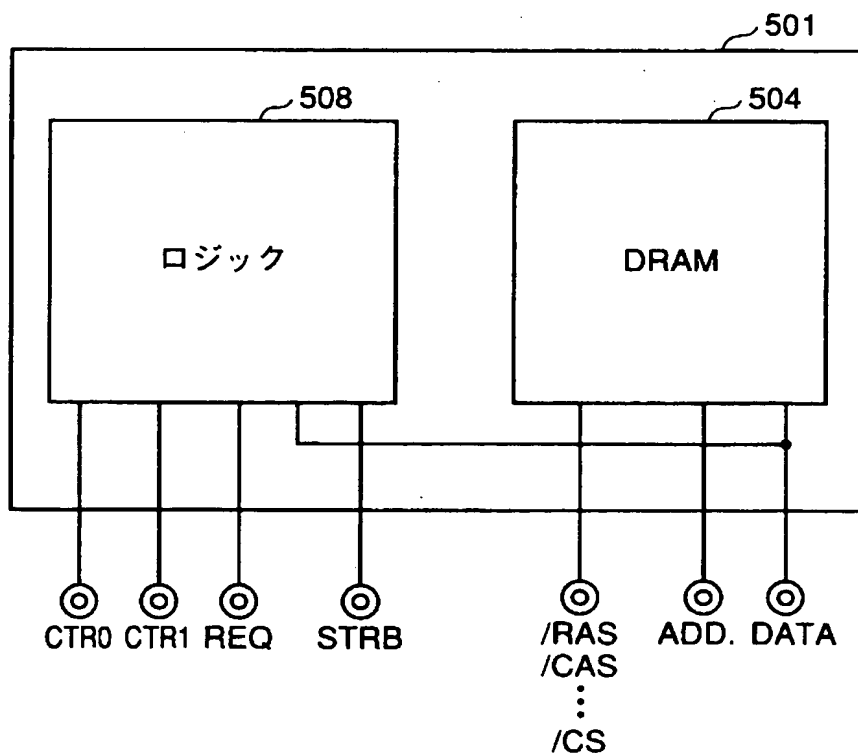
【図 5 3】



【図 5 4】

端子名	機能
CLK	マスタクロック
CKE	クロックイネーブル
/CS	チップセレクト
/RAS	行アドレスストローブ
/CAS	列アドレスストローブ
/WE	ライトイネーブル
DQ0~15	データ入出力
DQM(U/L)	出力ディスエーブル/ライトマスク
A0~11	アドレス入力
BA0,1(A12,13)	バンクアドレス
VDD	電源
VDDQ	出力用電源
Vss	接地
VssQ	出力用接地

【図 5 5】



【書類名】 要約書

【要約】

【課題】 マイコンシステムにおいて制御しやすいロジック内蔵 D R A M を提供する。

【解決手段】 インタフェース部 2 は、アドレス信号 A D D . で指定される領域が、ロジック制御領域である場合には、D R A M 4 とデータを授受する代わりに、レジスタ 6 とデータ授受を行なう。その際のデータ信号 D A T A は、レジスタ 6 に保持されるロジック回路 8 に対する制御コマンドや、処理のための入力データである。レジスタ 6 の保持内容に応じて、ロジック回路 8 は、たとえば、暗号処理や、画像処理等の、マイコンでは時間を要してしまう処理を実行する。処理結果はレジスタ 6 に保存され、D R A M に対する読出と同様のシーケンスで読出される。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000006013]

1. 変更年月日 1990年 8月24日

[変更理由] 新規登録

住 所 東京都千代田区丸の内2丁目2番3号

氏 名 三菱電機株式会社